VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÉ GRAFIKY A MULTIMÉDIÍ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER GRAPHICS AND MULTIMEDIA

SLEDOVÁNÍ POHYBU DAT NA MOBILNÍCH ZAŘÍZENÍCH

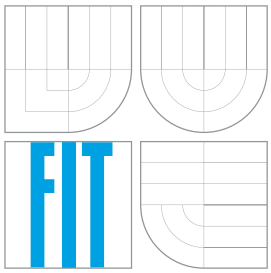
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

MARTIN ŠKOVIERA

BRNO 2012

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÉ GRAFIKY A MULTIMÉDIÍ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER GRAPHICS AND MULTIMEDIA

SLEDOVÁNÍ POHYBU DAT NA MOBILNÍCH ZAŘÍZENÍCH

TRACKING DATA ON MOBILE DEVICES

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — MARTIN ŠKOVIERA
AUTHOR

VEDOUCÍ PRÁCE — Ing. JAN NAVRÁTIL
SUPERVISOR

BRNO 2012

Abstrakt

Tato práce pojednává o možnostech sledování pohybu dat na mobilních zařízeních. Rozšiřuje čtenářovo povědomí o rozdělení trhu mobilních operačních systémů a důležitosti bezpečnostních řešení v podnikové sféře. Díky porovnání možností vývoje a bezpečnostních prvků platforem je ucelena představa o důležitosti těchto systémů. Součástí práce jsou vyvinuté aplikace na platformách Android a BlackBerry OS pro záznam sledovaných dat, serverová aplikace pro jejich sběr a iOS aplikace na PhoneLogs pro jejich hromadné zobrazení. Přístup k záznamům je možný až po úspěšné autentizaci, jednotlivé databáze jsou šifrovány a komunikace je zabezpečená SSL certifikátem.

Abstract

This thesis researches the possibilities of tracking mobile device data and their movement. It encompasses the division of the mobile operating systems market and also the importance of security solutions in business sector. Thanks to comparing the possibilities of development and security elements of individual platforms, the overview of importance is completed. The thesis also contains developed applications on Android and BlackBerry OS platforms for recording tracked data, a server application for their collection and a iOS application on PhoneLogs for their wholesale viewing. Accessing these records is possible after a successful authentication, individual databases are encrypted and communication secured with an SSL certificate.

Klíčová slova

Mobilní operační systémy, sledování komunikace, mobilní data, analýza trhu, porovnání platforem, Android, BlackBerry, iOS, kryptografie, SSL, Java, Objective-C, Python

Keywords

Mobile operating systems, communication tracking, mobile data, market analysis, platforms comparison, Android, BlackBerry, iOS, cryptography, SSL, Java, Objective-C, Python

Citace

Martin Škoviera: Sledování pohybu dat na mobilních zařízeních, bakalářská práce, Brno, FIT VUT v Brně, 2012

Sledování pohybu dat na mobilních zařízeních

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Ing. Jana Navrátila. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Martin Škoviera
12. května 2012

Poděkování

Tímto děkuji vedoucímu práce Ing. Janu Navrátilovi za korekturu technické zprávy a čas, který mně věnoval. Dále děkuji společnosti Safetica Technologies s.r.o., která mi poskytla odbornou pomoct, a Pavlu Krátkému za profesionální vedení.

Obsah

Kapitola 1

Úvod

Otázka sledovania pohybu dát na mobilných telefónoch je čím ďalej pálčivejšia. Je tomu hlavne z dôvodu nutnosti mať kontrolu nad citlivými dátami prenášanými zamestnancami. Táto práca pojednáva o spôsoboch sledovania komunikácie mobilných telefónov s jej okolím a o využití takéhoto riešenia v podnikovej sfére.

Informuje čitateľa o existencii jednotlivých mobilných operačných systémov vrátane ich trhového podielu a potenciálu. Opisuje akým spôsobom sa spoločnosti stavajú k problematike zabezpečenia a regulácie komunikácie ich zariadení. Práca si taktiež kladie za cieľ oboznámiť s možnosťami vývoja aplikácií na vybrané mobilné platformy s detailným opisom ich spôsobu zabezpečenia a limitov.

Bezpečnostné riešenie bude dostupné na troch mobilných operačných systémoch a komunikáciu bude riešiť vyvinutá serverová aplikácia. Bližšie priblíženie možnosti zaznamenávania pohybu dát je rozvedené o dôvody pre použitie jednej z opísaných metodík. Výber platforiem, na ktoré budú vyvinuté aplikácie vychádza z potenciálu ich nasledovného uplatnenia na trhu a teda komerčnej využiteľnosti v praxi.

Opísané sú rovnako aj jednotlivé fázy vývoja aplikácií a to od návrhu všetkých súčastí až po testovanie celého riešenia. Veľký zreteľ je kladený na spôsob a úroveň zabezpečenia jednotlivých úložísk a komunikácie medzi aplikáciami.

Využitie vyvinutých aplikácií je demonštrované na ukážkovom príklade s opisom možností nasadenia v praxi. Pre komerčné využitie sú rozvedené možnosti rozšírenia jednotlivých aplikácií ako aj celého riešenia. Poskytnutím manuálu na konfiguráciu a použitie aplikácií je uľahčená práca so zavedením vyvinutého bezpečnostného riešenia.

Kapitola 2

Mobilné operačné systémy

Mobilné telefóny dostupné v dnešnej dobe môžeme rozdeliť do dvoch kategórií, a to telefóny s proprietálnym operačným systémom dodaným výrobcom, taktiež známym pod anglickým výrazom „feature phone“, alebo „non smartphone“. Druhým typom sú mobilné telefóny s pokročilejším operačným systémom, tieto mobilné telefóny nazývame anglickým slovom „smartphone“. Hlavným problémom proprietálnych operačných systémov je podpora len pomerne limitujúcich platforiem ako Java a BREW[1].

Pokročilé operačné systémy na druhú stranu ponúkajú oveľa prijateľnejšie prostredie pre vývojárov aplikácií, ako dostupné programy na vývoj, ale aj možnosť využiť hardwarové prostriedky konkrétneho zariadenia cez dostupné rozhrania.

Za vývojom mobilných operačných systémov stoja rozličné firmy, či už výrobcovia hardware produktov, mobilných telefónov alebo software. Výrobcovia sa snažia, aby bol operačný systém vhodný ku každej príležitosti, do všetkých pracovných sektorov a na každú pracovnú pozíciu. Popularitu, meno a ohlas si prevažne získavajú spotrebiteľmi. Okrem mobilných telefónov sú mobilné operačné systémy vhodné aj pre tablety. Prácu s týmito zariadeniami obľubuje firemná sféra, či už pri právnických poradenstvách, marketingových poradách, hospitalizačných službách alebo mnoho iných, ako aj spotrebitelia pri každodennej zábave.

2.1 Priblíženie systémov

Symbian z dielne firmy Symbian Ltd. navrhnutý v roku 1998, je slobodný operačný systém, ktorý si našiel cestu k rade výrobcom mobilných telefónov. Jeho úspech a globálne nasadenie vyvrcholilo až k založeniu Symbian Foundation a prevziatie firmou Nokia v roku 2008. Každopádne odkúpenie mobilnej divízie Nokie firmou Microsoft v roku 2011 zapríčinilo pripravovaný prechod mobilných telefónov firmy Nokia zo systému Symbian na Windows Phone, ktorý vyvíja firma Microsoft. Podpora Symbianu na mobilných telefónoch Nokie je plánovaná do roku 2016.

iOS, ktorý od roku 2007 vyvíja firma Apple Inc., bol pôvodne známy pod názvom iPhone OS. Pretože firma ponúka na trhu viacero zariadení, využívajúce tento mobilný operačný systém, rozhodla sa ho pomenovať obecnejšie, názov taktiež zastrešuje produktovú radu firmy Apple. Uvedenie iPhone na trh zmenilo pohľad ostatných firiem, vývojárov, či dokonca historikov modernej doby.

[1] Binary Runtime Environment for Wireless

Google Inc., známa svojim internetovým vyhľadávačom, vstúpila na mobilný trh svojim operačným systémom Android v roku 2005 kúpou vývojárov z firmy Android Inc. Popularitu dokazuje fakt, že Android do svojich zariadení nasadilo veľké množstvo výrobcov mobilných telefónov. K dobrej povesti prispieva aj otvorenosť, ako má firma vo zvyku už od jej založenia.

Windows Phone bol predstavený firmou Microsoft v roku 2010 ako nástupca platformy Windows Mobile. Pričom predchodca bol určený pre podnikovú sféru, nová verzia prináša novú generáciu dizajnu a užívateľského prostredia a je hlavne určená pre spotrebiteľov. Tento mobilný operačný systém chce svoje ambície naplniť partnerstvom so spoločnosťou Nokia.

Proprietálny BlackBerry OS, používaný v telefónoch od spoločnosti RIM[2], je preslávený hlavne využívaním a nasadzovaním vo firemnom sektore po minulé roky. Spoločnosť je jedna z mála takých, ktorá navrhuje a vyrába mobilné telefóny, do ktorých používa vlastný operačný systém, čo dodáva istú úroveň komfortu z ponúkanej bezpečnosti. Už v roku 1999 vyrobila svoj prvý mobilný telefón a do kategórie smartphone sa zaradila v roku 2003.

WebOS ako pripravovaný produkt firmy Palm, prevzala v roku 2010 firma HP[3]. Operačný systém vychádza z Palm OS, ktorý bol predstavený v roku 2009. Okrem mobilných telefónov je pripravovaná podpora pre nasadenie na tablety, osobné a prenosné počítače tejto firmy.

MeeGo bol v roku 2010 predstavený ako spoločný projekt firiem Intel a Nokia. Berie si tie najlepšie vlastnosti z ďalej nevyvíjaných operačných systémov Maemo z dielne Nokie a Moblin od Intelu. Platforma je plne dostupná vývojárom po celom svete, preto vzniklo mnoho derivácií. Do určitej miery je systém určený aj pre malé prenosné počítače označované anglickým slovom „netbook“.

Platforma Bada, používaná vo vyšších radách mobilných telefónov spoločnosti Samsung, bola predstavená v roku 2009. Nejde o plnohodnotný operačný systém pre kategóriu smartphone, skôr sa táto platforma považuje za prechod medzi feature phone a smartphone.

Mobilné operačné systémy ako Android, WebOS, Maemo, Bada vychádzajú z Linux rodiny operačných systémov, iOS vychádza z operačného systému Mac OS X, ktorý je založený na BSD a NeXTSTEP [19] operačných systémov. Korene drvivej väčšiny moderných operačných systémov, poháňajúcich smartphone, siahajú až ku Unix. Avšak existujú ale aj ďalšie dostupné platformy, ako napríklad LiMo a Openmoko, ktoré sa ale v komerčnej sfére veľmi nepoužívajú.

2.2 Tržné postavenie platforiem

Situácia na poli mobilných telefónov sa neustále dynamicky mení. Vznikajú a zanikajú nové operačné systémy, výrobcovia mobilných telefónov prechádzajú na nové platformy, prípadne ich sami rozvíjajú. Pre množstvo mobilných operačných systémov dostupných na trhu je nutné demograficky analyzovať celosvetový trh.

Touto analýzou získame potrebné informácie na výber najvhodnejších mobilných operačných systémov, ako aj platforiem. Taktiež analyzujeme trendy, aby sme lepšie dokázali odhadnúť, aká bude situácia v čase dostupnosti aplikácie určenej pre trh.

[2] Research In Motion
[3] Hewlett – Packard

2.2.1 Segmentácia spotrebiteľov

Trh pre mobilné telefóny sa empiricky rozdeľuje na produkty využívané spotrebiteľmi a firmami. Situácia na trhu je pre obe kategórie odlišná, vyplýva to od potrieb spotrebiteľov a firiem pri ich každodenných činnostiach. Podiel predaných mobilných telefónov spadajúcich do kategórie múdrych telefónov [1] je iba 27 %.

Ak nebudeme uvažovať zakúpené mobilné telefóny spotrebiteľmi a zameriame sa na firemnú sféru, kde sú výrazne iné požiadavky na platformu, zistíme podľa najnovších prieskumov [7], že až dve tretiny firiem dávajú svojim zamestnancom práve smartphone.

Pracovná doba je často dynamická, odhaduje sa, že v priemere 20 % času zamestnanci trávia počas svojej pracovnej doby mimo ich pracovnej stanice či pracoviska a potrebujú aj v danú chvíľu efektívne pracovať. Možnosť využívania smartphone je nutná hlavne pre

- obchodné vedenie pre možnosť rozhodovania sa na cestách
- predajca má možnosť kontaktovať klienta a vybavenie objednávky
- pracovník personálnej oblasti podpory pre prístup k informáciám klientov
- technickí pracovníci v teréne alebo pracovníci pracujúci na diaľku
- zamestnanci počas prezentácií, konferencií, školení či pracovných porád

So zavedením smartphone prichádzajú možné komplikácie a výzvy pre spoločnosti, ako aj pre jednotlivých zamestnancov. Viacero smartphone na pracovisku prináša zvýšenie záťaže siete a dátovej linky danej spoločnosti, ako aj prípadne nové nároky na dáta prístupné v reálnom čase pre povahu mobilných telefónov.

Ako je ďalej opísané v kapitole 3.3, spoločnosti musia uvážiť nové riziká zavedením smartphone na pracovisko. Po minulé roky bola problémom aj fragmentovanosť bezdrôtových zariadení, prístupových bodov a bezdrôtových štandardov, každopádne niektoré firmy prechodom na smartphone inovujú celú firemnú infraštruktúru, ktorú musia dodatočne otestovať a zaškoliť zamestnancov. Smartphone by taktiež mali byt kompatibilné so súčasnou infraštruktúrou a požadovanými politikami prístupu. Nutnosťou je aj možnosť hromadnej správy týchto zariadení.

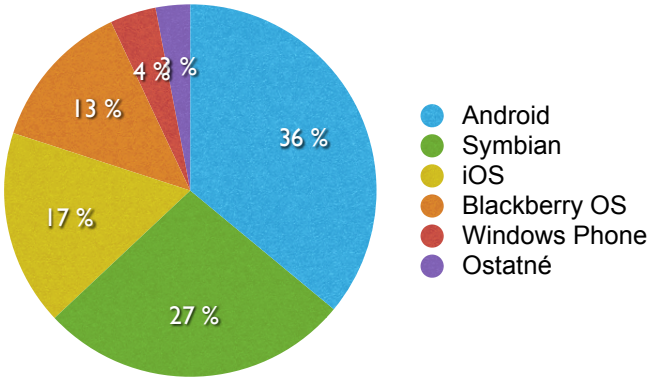
2.2.2 Analýza trhu

Každý mobilný operačný systém má svoje zázemie, ktoré mu pomáha vybudovať výrobca mobilných telefónov, ktorý daný operačný systém nasadzuje do svojich produktov. Do istej miery popularita platformy závisí na danom prevedení mobilného telefónu, jeho značky, dizajnu a funkcionalít, ako to pociťujú hlavne spotrebitelia. Pre firmy je ale podstatnejšie využitie daného operačného systému a jeho možnosti zabezpečenia pri každodennej práci. Preto si získali mobilné operačné systémy podiel na trhu, ktorý môže byt odlišný na kontinentoch či jednotlivých krajinách.

Každým rokom sa celosvetový podiel mobilných operačných systémov mení, či už po príchode nových populárnych modelov mobilných telefónov používajúcich tieto operačné systémy, alebo majoritných nových verzií a vylepšení platformy, či už pre vývojárov alebo koncového zákazníka.

Momentálne dostupné operačné systémy prišli na trh v iných časových obdobiach a preto mohli mať skoršie uvedené systémy náskok pred neskoršie uvedenými. Vďaka časovým rozdielom je ale možné pozorovať popularitu, rýchlosť adaptácie a trendy jednotlivých operačných systémov na celosvetovom trhu.

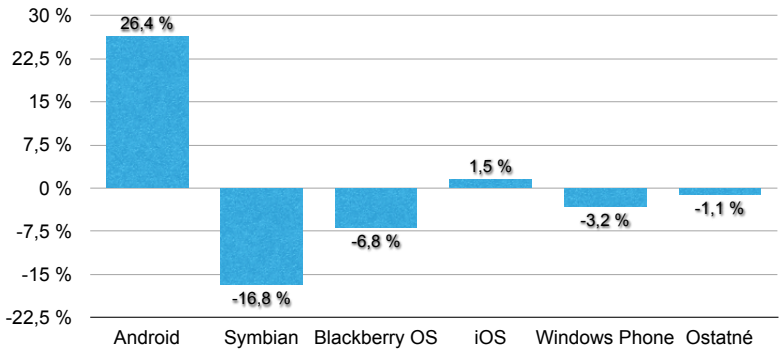
Podľa najnovších štúdií [15] spotrebiteľského a firemného odberu, dominuje trhu mobilný operačný systém Android, ako je to uvedené na obrázku 2.1.



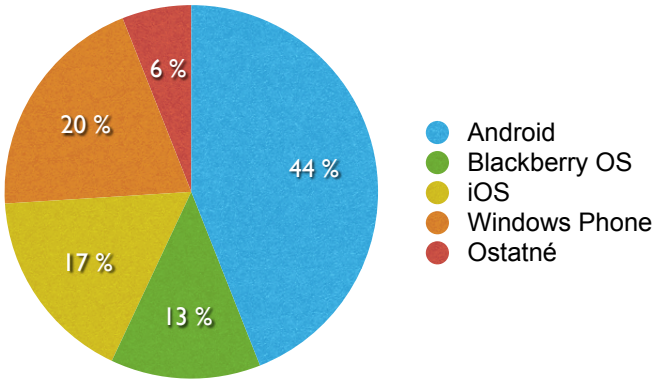
Obr. 2.1: Podiel mobilných operačných systémov na celosvetovom trhu

Ako už bolo spomenuté, pre vývoj a komerčný prehľad je podstatný trend ako jednotlivé mobilné operačné systémy budú pokračovať na celosvetovom trhu. Ročný nárast trhových podielov od prvého kvartálu roku 2010 jednotlivých systémov je uvedený na obrázku 2.2.

Spojením mobilnej divízie firmy Microsoft s Nokiou a vypustenie podpory mobilného operačného systému Symbian v roku 2016 a nahradením operačným systémom Windows Phone, sa odhaduje [16], že podiel Windows Phone v spotrebiteľskom odbere bude 20 % ako je vidieť na obrázku 2.3.



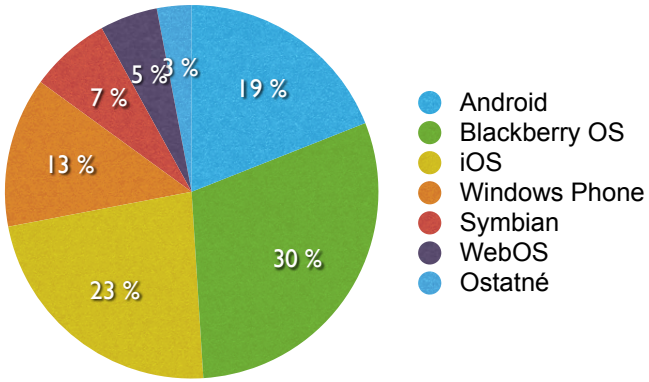
Obr. 2.2: Ročný nárast podielu mobilných operačných systémov



Obr. 2.3: Odhady odberu pre spotrebiteľský trh v roku 2015

Situácia vo firemnom sektore je ale podstatne iná. Firmy vlastnia viacero modelov mobilných telefónov a podporujú rozličné platformy. Aktuálnu situáciu rozdelenia trhu vo firemnom sektore ukazuje obrázok číslo 2.4, ako dokazuje najnovší prieskum [7].

Vrcholných 500 spoločností podľa rebríčka Fortune [9] sa vyjadrilo, že je pre nich najväčším lákadlom operačný systém iOS, ktorý by chceli v budúcnosti podporovať.



Obr. 2.4: Podiel podporovaných mobilných operačných systémov v podnikovej sfére

2.3 Dominantné systémy

Z analýzy celosvetového trhu, trhu na jednotlivých kontinentoch a využitím v jednotlivých odvetviach priemyslu sme sa dozvedeli, že mobilné operačné systémy Android a iOS majú sľubnú budúcnosť a veľmi rýchlo si získavajú čoraz väčší podiel na trhu. Je tomu tak pre ich využiteľnosť v podnikovej sfére, ako aj vďaka spotrebiteľskej popularite.

Mobilný operačný systém iOS má najsilnejšie zastúpenie v Severnej Amerike, kde v Spojených štátoch Amerických bol doposiaľ iPhone predávaný iba jedným mobilným operátorom a to spoločnosťou AT&T. Situácia sa koncom prvého kvartálu roku 2011 zmenila, pretože tento mobilný telefón začal ponúkať aj ďalší operátor a to Verizon. V súčastnosti je taktiež v ponuke operátora Sprint.

Dôkazom nefragmentovanosti tejto platformy je aj fakt, že po predstavení novej verzie operačného systému iOS 5 na konferencii WWDC2011[4] až 94 % užívateľov má nainštalovanú najnovšiu majoritnú verziu. Je v záujme spotrebiteľov a spoločností, aby ich zariadenia mali najnovšie verzie operačných systémov, ktoré pridávajú novú funkcionalitu a zlepšujú stav bezpečnosti zariadenia. Tento fakt majitelia rešpektujú a je to dôkazom, že mobilný operačný systém iOS verzie 2 má iba 1 % majiteľov.

Podiel a rozloženie mobilného operačného systému Android, je do veľkej miery daný mobilnými telefónmi, ktoré tento systém používajú. O distribúciu sa hlavne starajú modely firmy HTC, ktoré reprezentujú 53 % predaných telefónov platformy Android, na druhom mieste sú modely spoločnosti Motorola s 30 % podielom. Tieto dve spoločnosti vykazujú veľké obraty a predaje hlavne v Severnej Amerike. Na ázijskom trhu je populárna spoločnosť Samsung, ktorá ale do svojich zariadení nasadzuje viacero mobilných operačných systémov a k nie príliš vysokému podielu na ázijskom trhu prispieva aj fakt, že služby spoločnosti Google nie sú v Ázii natoľko populárne ako v Amerike alebo v Európe.

Platforma Android pociťuje fragmentáciu oveľa silnejšie ako tomu je u konkurenčnej platformy iOS. Už minoritné zmeny v číslovaní prinášajú veľmi veľké zmeny a preto je fragmentácia problémom pre vývojárov aplikácií na túto platformu. Okrem aktuálne nasadzovanej verzie Froyo, existujú na trhu a tým pádom aj v zariadeniach nainštalované staršie verzie s pomerne vysokým podielom.

Operačný systém Symbian má na ázijskom trhu najväčší podiel [21], ale je na ústupku a stráca podiely po celom svete.

2.4 Pohľad vývojárov

Pri výbere platformy podľa hodnotenia trhu, zamerania firmy, prípadne daného produktu, si treba uvedomiť a zhodnotiť, ako dané platformy vnímajú ostatní vývojári, kde je vysoká konkurencia, aká je úspešnosť produktov a ako sú daní vývojári spokojní s vývojom pre daný mobilný operačný systém.

Podľa vyjadrení vývojárskych spoločností [18] celkom 47 % vývojárov podporuje viac ako jednu platformu a to konkrétne Android má zastúpenie v 68 % dotazovaných vývojárskych spoločností a platforma iOS v 54 %. Na druhú stranu Symbian a BlackBerry OS dosiahli pod 20 % podiel. Ďalej podľa zistení až 70 % vývojárov platformy iOS chce v blízkej budúcnosti pridať podporu svojich produktov pre mobilný operačný systém Android, zatiaľ čo naopak tomu je iba pri 48 % vývojárov.

[4] Každoročná konferencia usporiadaná firmou Apple určená pre vývojárov

Najviac spokojní s platformami sú vývojári iOS a Androidu, kde na druhej strane, najväčšiu nespokojnosť pociťujú vývojári BlackBerry OS. Každopádne pri výbere platformy treba brať zreteľ na viacero faktorov. Jedným z nich môže byť práve doba potrebná na naučenie sa a spoznanie danej platformy. Nezáleží iba od jazyka, v ktorom sa programuje pre danú platformu, ale aj dostupné vývojárske a ladiace nástroje, či vývojárske balíčky sú významné. Najmenej času potrebujú vývojári pre adaptáciu na mobilný operačný systém Android, ktorý pre svoje kvality a ponúkané nástroje minimalizuje problémy, spôsobené fragmentáciou platformy. V tesnom závese je platforma iOS a Windows Phone 7. Zdroje často neuvádzajú, ale veľmi fragmentovaným operačným systémom je aj BlackBerry OS, ktorý si vyžaduje dvojnásobnú dĺžku pozornosti ako konkurenčný Android. Najmenej prívetivejší mobilný operačný systém pre spoločnosti, ktoré chcú pridať podporu tejto platformy je Symbian, vyžaduje totiž trojnásobok času.

Rozloženie vývojárskych firiem môžeme určiť vďaka geolokačným analýzam [3]. Európa svojím 41 % zastúpením prevyšuje Severnú Ameriku a Áziu dvojnásobkom. V prípade zamerania sa na spoločnosti, ktoré vyvíjajú mobilné aplikácie či riešenia, treba vedieť, na ktorom trhu pôsobia. Za zmienku stojí aj fakt, že spoločnosti so zameraním na vývoj aplikácií si musia chrániť svoje intelektuálne vlastníctvo, pretože percento zamestnancov, ktorí majú prístup k týmto informáciám je podstatne vyššie ako u bežných spoločností.

2.5 Vývoj na platformách

Pred začatím vývoja a práce na aplikácii či inom špecifickom riešení určenom na mobilné platformy je nutné porovnať vybrané mobilné operačné systémy.

Z analýzy trhu vieme zastúpenie platforiem na mobilnom trhu a verzie jednotlivých operačných systémov nasadených v mobilných telefónoch vo firemnom sektore. V tejto analýze porovnáme päť najvýznamnejších mobilných operačných systémov ako Symbian, Windows Phone podporovanými výrobcom Nokia, Android ako voľne licencovateľný systém od firmy Google, iOS nasadzovaný do mobilných zariadení firmy Apple a BlackBerry OS, najznámejší mobilný operačný systém pre spoločnosti od firmy RIM.

Vývoj aplikácií na jednotlivých mobilných operačných systémoch často uľahčujú vývojárske balíčky, označované skratkou „SDK“. Pri návrhu aplikácie je treba vziať do úvahy tieto balíčky, naštudovať ich a prispôsobiť im prípadne koncept aplikácie. Tieto vývojové balíčky sú odlišné nie len jazykom, ktorým sú napísané, ale aj podporovanými operačnými systémami, na ktorých môže byť uskutočnený vývoj.

2.5.1 Operačné systémy

Prístup ku jednotlivým vývojárskym balíčkom môže byť limitovaný na operačné systémy, na ktorých jednotlivé balíčky môžu byť spustiteľné. O aké systémy konkrétne ide je uvedené v nasledujúcej tabuľke číslo 2.1.

Systém	Android	iOS	BlackBerry OS	Windows Phone	Symbian
Windows	Áno	Nie	Áno	Áno	Áno
Linux	Áno	Nie	Áno	Nie	Áno
Mac OS X	Áno	Áno	Áno	Nie	Áno

Tabuľka 2.1: Operačné systémy, pod ktorými je možný vývoj pre dané platformy

2.5.2 Poplatky

Pre prístup k vývojárskym dokumentáciám či balíčkom platia pre mobilné operačné systémy rôzne pravidlá a podmienky. Vo väčšine prípadov je nutná registrácia na vývojárskych stránkach daných mobilných operačných systémoch. Ani jedna z porovnávaných platforiem nedisponuje nutnosťou platenej registrácie, každopádne poplatky za ďalšie služby, ako distribúcia či možnosť inštalácie na mobilné zariadenia, sa vyskytujú. Pojednáva o tom tabuľka číslo 2.2.

Licencie	Android	iOS	BlackBerry OS	Windows Phone	Symbian
Suma	$ 25	$ 99	Zadarmo	Zadarmo	1 €
Poplatok	Len raz	Ročný	Nepotrebný	Nepotrebný	Len raz
Distribúcia	Play	App Store	App World	Marketplace	Ovi Store

Tabuľka 2.2: Poplatky za licencie jednotlivých platforiem

2.5.3 Jazyky

Každý mobilný operačný systém moderných smartphonov, podporuje spúšťanie aplikácií tretích strán. Tieto aplikácie sa programujú v tých istých jazykoch, ktorých spúšťanie podporuje daný operačný systém. Tabuľka číslo 2.3 zobrazuje programovacie jazyky, ktoré sú jednotlivými operačnými systémami podporované pri vývoji aplikácií.

Jazyk	Android	iOS	BlackBerry OS	Windows Phone	Symbian
Java	Áno	Nie	Áno	Nie	Áno
C #	Nie	Nie	Nie	Áno	Áno
C/C++	Áno	Nie	Áno	Nie	Áno
Objective-C	Nie	Áno	Nie	Nie	Nie

Tabuľka 2.3: Programovacie jazyky podporované danými platformami

2.5.4 Ladenie a emulácia

Testovacie a ladiace nástroje sú potrebné pri vyvíjaní aplikácií, každopádne nie vždy je výhodné testovať aplikáciu na mobilnom telefóne, či už z dôvodu absencie počtu zariadení, alebo rýchlosti testovania a ladenia danej aplikácie. Z dôvodu, že existuje viacero mobilných operačných systémov naprogramovaných v rôznych programovacích jazykoch, s oficiálnou podporou vývojárskych balíčkov a nástrojov na rôznych operačných systémoch, tak neexistuje univerzálny emulátor týchto mobilných operačných systémov.

Preto záleží od vývojárov daných mobilných operačných systémov. Pre použitie známych programovacích jazykov je podpora editorov na dobrej úrovni. Niektoré editory podporujú aj vzdialené ladenie aplikácie spustenej v mobilnom telefóne. V tabuľke číslo 2.4 je vidieť, ako emulátory prostredí nie sú dostupné na tých istých operačných systémoch, ako je možný ich vývoj.

Systém	Android	iOS	BlackBerry OS	Windows Phone	Symbian
Windows	Áno	Nie	Áno	Áno	Áno
Linux	Áno	Nie	Nie	Nie	Nie
Mac OS X	Áno	Áno	Nie	Nie	Nie

Tabuľka 2.4: Dostupnosť emulátorov mobilných operačných systémov

2.6 Vybrané platformy

Analýzou a porovnaním vybraných mobilných operačných systémov sme získali poznatky o vybavenosti systémov, pripravenosti začlenenia do podnikovej sféry spoločne s požiadavkami na vývoj na danej platforme. Spoločne s analýzou trhu mobilných operačných systémov môžeme odhadnúť či predpovedať budúci podiel platforiem v podnikovom sektore.

Ako vyplýva z predchádzajúcich kapitol, mobilné operačné systémy Android, BlackBerry OS a Symbian dávajú vývojárom možnosti a prostriedky pre realizáciu komplexných bezpečnostných zabezpečení. Na druhú stranu operačné systémy iOS a Windows Phone v aktuálne dostupných verziách neprinášajú vývojárom tak pokročilé možnosti správy systému, ako by pre bezpečnostnú aplikáciu bolo žiadané. Preto sú pre iOS poskytnuté prostriedky pre pokročilé zabezpečenie prostredia v aplikáciach, ktoré je možné akcelerovať hardware podporou. Pre absenciu multitaskingu v operačnom systéme Windows Phone, ktorá môže byť pridaná v budúcnosti, nie je možné komplexne pomyslieť na bezpečnostnú aplikáciu vynímajúc chránenia a správy aplikačných dát.

Pre účely sady vyvíjaných aplikácií poslúžia mobilné operačné systémy iOS, Android a BlackBerry OS.

Kapitola 3

Bezpečnosť platforiem

Pre ochranu osobných, korporátnych informácií a identity na jednotlivých mobilných operačných systémoch, je potreba vedieť, proti čomu sa treba chrániť. Pre rozmery sú mobilné telefóny náchylnejšie na stratu či odcudzenie zariadenia. Nami porovnávané mobilné operačné systémy disponujú rôznymi ochranami či možnosťami zabezpečenia mobilných telefónov.

Na základe predstavenia pojmov bezpečnosti, s ktorými sa téma mobilných operačných systémov potýka, je možné bližšie pochopiť a vysvetliť ich teóriu. Miera bezpečnosti analyzovaných platforiem sa od seba odlišuje, každopádne vždy je založená na tých istých princípoch a je ich možno porovnať rovnakými metódami.

Preto základnými kritériami bezpečnosti komunikácie sú

- **utajenie** – poslucháč na kanále dátam nerozumie
- **autentizácia** – odosielateľ je tým, za koho sa vydáva
- **integrita** – istota, že dáta neboli na ceste modifikované
- **nepopierateľnosť** – zdroj dát nemôže poprieť ich odoslanie

3.1 Kryptografia

Kryptografia je veda, zaoberajúca sa procesom udržiavania informácií v bezpečí využitím šifrovania a dešifrovania. Spoločne s kryptoanalýzou patrí pod vedný obor kryptológia. Zabezpečenie šifrovacieho algoritmu je možné buď jeho utajením alebo zavedením kľúčov, ktoré parametrizujú daný algoritmus [6]. V prípade veľkého množstva kľúčov je možné, aby bol algoritmus verejne známy.

Transformáciu nechránených dát do chránenej zašifrovanej podoby vykonáva kryptografický systém. Všetky transformácie sú vykonávané s príslušným kryptografickým algoritmom a použitím kľúčov. Kryptografický systém je potom parametrický systém kryptografických transformácií [20]

$$T^K = (Tk : k \varepsilon K), \text{ kde } k \text{ je kľúč a } K \text{ je priestor kľúčov}$$

3.1.1 Symetrická kryptografia

Symetrické kryptografické systémy sú založené na skutočnosti, že ako odosielateľ tak aj príjemca disponuje rovnakým tajným kľúčom. Implementácia takýchto algoritmov býva efektívna, často aj s možnosťou hardwarovej akcelerácie. Problém býva s distribúciou tajného

kľúča, pretože odosielateľ nemôže zaručiť, že kľúč cestou nebude zachytený neautorizovanou osobou. Medzi známe algoritmy pre symetrickú kryptografiu patrí dnes už prekonaný DES, jeho varianta 3DES a populárny AES.

Algoritmus s názvom Rijdael [5] sa stal schválenou šifrou pod názvom AES ako federálny štandard. Nahrádza starý štandard DES s novou podporou dĺžok kľúčov a to 128, 192, alebo 256 bitov. V súčasnej dobe postačuje dĺžka kľúča 128 bitov a paradoxne za určitých podmienok je 256 bitový kľúč menej bezpečný[1]. AES je blokový šifrovací algoritmus, ktorý je aplikovateľný na dáta s pevnou dĺžkou 128 bitov. Dáta s väčšou dĺžkou sú spracovávané po jednotlivých blokoch. Pokiaľ dĺžka nezodpovedá vyžadovanému násobku, musia byť rozšírené na potrebnú dĺžku. Existuje na to niekoľko algoritmov, od jednoduchého doplnenia dát až po pokročilé schémy ako tomu je pri najpoužívanejšom mechanizme PKCS #7 [12].

Aby nebola kompromitovaná bezpečnosť šifry tým, že budú jednotlivé bloky šifrované za sebou, využíva sa napríklad algoritmus CBC[2]. Funguje spôsobom, že daný blok je pred šifrovaním vystavený procesu exkluzívnej disjunkcie s predchádzajúcim blokom. Z dôvodu, že prvý blok nemá žiaden blok k dispozícii, je nutné využiť inicializačný vektor. Dôležité je, aby boli inicializačné vektory vždy generované. Z bezpečnostného hľadiska, znalosť inicializačného vektoru nenapomáha útočníkovi prelomiť šifru.

3.1.2 Asymetrická kryptografia

Hlavným rysom asymetrickej kryptografie je existencia párových kľúčov. Dáta zašifrované jedným z kľúčov je možné dešifrovať iba tým druhým. Využívajú sa k tomu dva kľúče, a to verejný a súkromný. Ide o výpočetne náročnejší spôsob šifrovania, preto sa využíva hlavne na predávanie generovaných kľúčov pre symetrickú kryptografiu, ako aj pre elektronický podpis. Najznámejším využívaným symetrickým mechanizmom je algoritmus RSA.

Ide o prvý algoritmus pre asymetrickú kryptografiu, ktorý je vhodný pre šifrovanie a podpisovanie. Pri dostatočnej dĺžke kľúča je považovaný za bezpečný. Algoritmus RSA funguje [4] tak, že pomocou dvoch náhodne generovaných prvočísiel p a q, vygeneruje dvojicu kľúčov. Bezpečnosť je založená na predpoklade, že rozložiť číslo na súčin prvočísiel $n = p * q$ je časovo a výpočetne náročná úloha. Kľúče sú typicky dlhé 1024 až 2048 bitov so špecifickými požiadavkami na generované prvočísla podľa štandardu PKCS #1 [11].

3.1.3 Certifikát

Pre možnosť riešenia problému uchovávania, distribúcie a správy kryptografických kľúčov, bol zavedený pojem certifikát verejného kľúča. Ide o digitálne podpísanú dátovú štruktúru, ktorá obsahuje verejný kľúč spoločne s údajmi pre jednoznačnú identifikáciu držiteľa certifikátu. Pre kompatibilitu vydávaných certifikátov, existuje rada noriem popisujúcich štruktúru certifikátu, ako napríklad X.509 [10]. Pre potrebu podpisov certifikátov dôveryhodnými stranami existuje rada spoločností a inštitúcií, ktoré sa považujú za certifikačné autority.

3.1.4 Kryptografická hašovacia funkcia

Ide o funkciu pre prevod ľubovoľné dlhého vstupného reťazca na výstup pevnej dĺžky, ktorá je závislá od použitého hašovacieho algoritmu. Pre rýchlosť algoritmu môže slúžiť ku kontrole integrity dát, indexovaniu, vyhľadávaniu, či kontrolu pravosti.

[1] Opis bezpečnosti 256 bitového kľúča je dostupný na adrese http://eprint.iacr.org/2009/374
[2] Cipher Block Chaining

Požiadavky kladené na kryptografickú hašovaciu funkciu obsahujú taktiež nároky bežnej hašovacej funkcie. Spoločne sú to teda požiadavky ako

- **rýchlosť transformácie** – funkcia rýchlo zo vstupu spočíta požadovaný výstup
- **rozloženie výstupov** – rovnomerná distribúcia výstupov pre nízky počet kolízií
- **lavínovitosť** – zmena jediného bitu vstupu produkuje odlišný výstup
- **jednocestnosť** – znalosť výstupu nevedie k znalosti vstupu
- **silná bezkolíznosť** – nemožnosť nájdenia dvoch vstupov s rovnakým výstupom
- **slabá bezkolíznosť** – nemožnosť nájdenia vstupu, ktorý bude mať rovnaký výstup ako vstup, ktorého výstup už poznáme

Medzi najznámejšie kryptografické hašovacie algoritmy radíme 128 bitový MD5 a rodinu SHA algoritmov. Kľúče závisia na použitej variante a to od 160 až po 512 bitov.

3.2 Šifrované spojenie

Pre možnosť zabezpečenej komunikácie šifrovaním a autentizáciou komunikujúcich strán boli vyvinuté protokoly SSL[3] a neskorší TLS[4]. Ide o protokoly, ktoré kombinujú symetrickú a asymetrickú kryptografiu. Z hľadiska OSI modelu ich zaradenie je v relačnej a prezentačnej vrstve, teda medzi transportnú a aplikačnú vrstvu podľa modelu TCP/IP.

Autentizácia komunikujúcich strán je na relačnej vrstve a zašifrované segmenty sú na vrstve transportnej. Táto autentizácia je spravidla na základe certifikátu serveru, ktorý je šifrovaný pomocou asymetrickej kryptografie a prenos dát je šifrovaný symetricky.

3.2.1 Virtuálna privátna sieť

Pre povahu mobilných zariadení nie je možné sa pripájať do siete spoločnosti len pomocou zabezpečenej firemnej siete. Ide preto o prostriedok k prepojeniu viacero zariadení v sieti internet, známy pod skratkou VPN. Zariadenia musia mať možnosť medzi sebou komunikovať rovnakým spôsobom, ako by tomu bolo v prípade použitia firemnej siete.

Totožnosť jednotlivých strán je overovaná za pomoci certifikátov a komunikácia je následovne šifrovaná. V firemnej sieti je nutná prítomnosť VPN serveru, ktorý je pripojený k verejnému internetu a pre svojich klientov zabezpečuje funkcionalitu sieťovej brány s poskytovaním intranetu formou sieťového tunelovania. Autentizácia certifikátom, okrem iného dáva možnosť využitia takzvaného „VPN on Demand“, ktorý robí VPN autentizačný proces transparentným, zatiaľ čo stále poskytuje zabezpečený prístup k podnikovým službám.

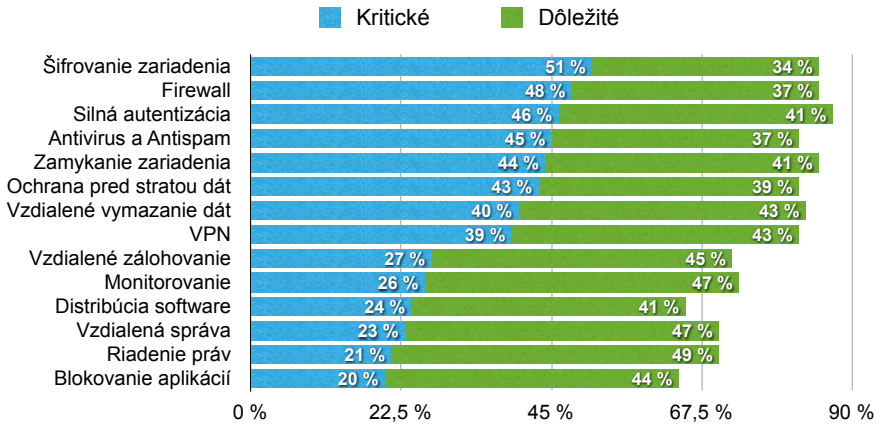
[3] Secure Sockets Layer
[4] Transport Layer Security

3.3 Potreba bezpečnosti

Citlivé informácie uložené v mobilných telefónoch treba chrániť, tento fakt si uvedomujú aj firmy [7], pretože až 80 % firemných dokumentov je uložených v emailovej komunikácii alebo na intranete a práve 83 % zamestnancov má prístup k internetu z mobilného telefónu.

Po odcudzení mobilného zariadenia môžu vzniknúť úniky firemných údajov tretím stranám, odcudzenie prístupových kódov, alebo aj dokonca krádeže identity. Tieto straty dát môžu znamenať nepredstaviteľný problém pre danú firmu, pretože niektorí zamestnanci majú prístup ku privátnym dátam spoločnosti.

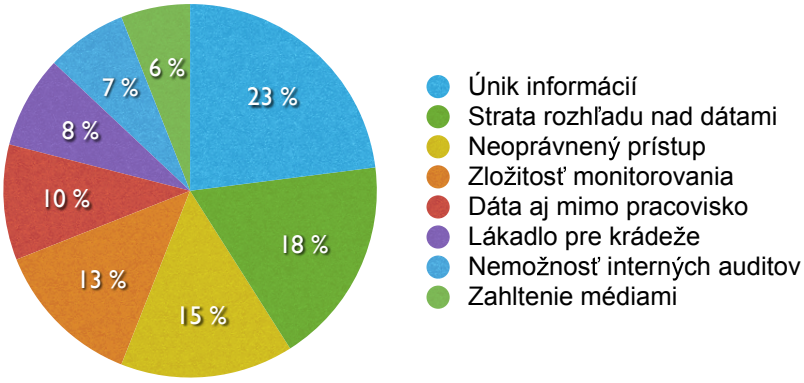
Využiť všetky dostupné prostriedky na zabezpečenie a minimalizáciu možných bezpečnostných problémov je finančne, časovo a kapacitne náročné [14]. Nasledujúca tabuľka 3.1 preto vystihuje, aké sú kladené nároky na bezpečnostné aplikácie či možnosti mobilného operačného systému. Po adoptovaní smartphone do firemnej sféry firmy taktiež zaznamenávajú konkrétne problémy, s ktorými sa musia vysporiadať. Najväčším problémom ako monitorovať či chrániť únik informácií z mobilného telefónu dokazuje aj obrázok 3.2.



Obr. 3.1: Kladené nároky na platformu

Ďalej podľa analýz a vyjadrení firiem [7]

- 46 % zamestnancov v práci používa vlastný nezabezpečený mobil
- 33 % zamestnancov sa neprihlasuje cez VPN aj keď ju majú dostupnú
- 85 % zamestnancov sa pripája na nezabezpečené WiFi siete počas cestovania
- 31 % zamestnávateľov vyžaduje nainštalovaný bezpečnostný software
- 32 % zamestnávateľov školí svojich zamestnancov



Obr. 3.2: Jednotlivé problémy spojené so zavedením smartphone

3.4 Stav bezpečnosti platforiem

Hlavné bezpečnostné riziká a problémy môžeme rozdeliť do troch kategórií, a to

- osobné informácie a dáta uložené na mobilnom telefóne v dobe odcudzenia, straty alebo servisných zásahov
- odchytávanie citlivých informácií pri nezabezpečenom pripojení na internet
- možnosť spúšťania škodlivého kódu vďaka bezpečnostným zraniteľnostiam mobilného operačného systému či v aplikáciach

Niektorým hrozbám sa dá aktívne brániť po zavedení danej platformy do infraštruktúry spoločnosti, každopádne sa nedá vždy minimalizovať riziko odcudzenia či straty mobilného zariadenia a preto by mal byť mobilný operačný systém na takú situáciu pripravený. Práve pri strate či odcudzení by mohla mať nepovolaná osoba prístup ku

- kalendárom, schôdzkam a kontaktom
- pracovným a osobným dokumentom, poznámkam a emailom
- účtom, ku ktorým má mobilný telefón prístup
- aplikáciám, ktoré môžu obsahovať citlivé informácie, alebo k ním dokážu pristúpiť
- prístupu na bezdrôtovú sieť v spoločnosti či v domácnosti
- prístupu do vnútornej siete spoločnosti

Pri nedostatočnom zabezpečení siete je možné útočníkmi odchytávať neoprávnené informácie. Problémy taktiež spôsobujú nešifrované spojenia so vzdialenými servermi, stránkami či službami. Nutnosťou sú aj aktualizácie mobilných operačných systémov na aktuálne verzie podporované výrobcami. V prípade bezpečnostných zraniteľností môže byť ohrozený mobilný telefón

- manipuláciou nastavení vedúcim až na nemožnosť používania mobilného telefónu s potrebou obnovy systému
- odcudzením prípadne zničením korporátnych a osobných informácií
- využitím mobilného telefónu za účelom obohatenia útočníka posielaním správ či vytáčaní prémiových platených telefonických čísiel
- použitím mobilného telefónu na rozosielanie nevyžiadanej pošty a dotazov na vzdialené servery

3.4.1 Kritériá bezpečnosti

Pre objektívne porovnanie mobilných operačných systémov a ich možností nasadenia do podnikovej sféry je potreba si stanoviť kritériá hodnotenia. Nami porovnávané operačné systémy majú momentálne stále aktívne vývojárske zázemie, niektoré z nich sú mladšie a neponúkajú také možnosti ako iné, no tento fakt sa časom môže zmeniť.

Citlivé informácie

Prvou líniou obrany je možnosť zabezpečiť mobilný telefón heslom, ktoré je žiadané vždy pri spustení zariadenia, odomykania, prípadne v ďalších situáciách. Tento spôsob ochrany ale nezabráni pokročilejším útočníkom pristúpiť ku citlivým informáciám, dostupným na danom mobilnom telefóne.

Pre ochranu dát na mobilnom telefóne je potrebné mať dáta uložené v zašifrovanej podobe, najlepšie na úrovni mobilného operačného systému s podporou hardware akcelerácie. Citlivé informácie ako heslá, certifikáty či informácie o účtoch, je najlepšie ukladať v osobitnej aplikácií, ktorá svoj obsah šifruje a vyžaduje unikátne prístupové heslo. Dôležitým faktorom je taktiež možnosť pravidelného zálohovania pre prípady porúch a následné odoslanie mobilného telefónu technickej podpore, ako aj možnosť túto zálohu efektívne šifrovať.

V prípade, že už bol mobilný telefón stratený či odcudzený, záleží na mobilnom operačnom systéme, či podporuje jeho nájdenie a vzdialené vymazanie obsahu tohto zariadenia. Pokiaľ dané zariadenie nie je možné vyhľadať a následne vymazať jeho obsah na diaľku, podpora automatického vymazania po určitom počte chybne zadaných kombinácií hesla je vítaná.

Zraniteľnosti

Mobilné operačné systémy, ako každý iný produkt podlieha náchylnostiam na zraniteľnosti či už sú verejne známe alebo nie. Vývojárske tímy tieto chyby priebežne opravujú, preto je nutnosťou aktualizovať na nové verzie mobilného operačného systému, ktoré tieto chyby napravujú. Rovnako bezpečnostné zraniteľnosti môžu obsahovať aj aplikácie tretích strán, prípadne môžu byť inštalované podvodné verzie aplikácií, preto by mali byť tieto aplikácie inštalované iba z dôveryhodných zdrojov prípadne s certifikátmi.

Niektorých zraniteľností využívajú procesy nazývané „jailbreak“ a „rooting“, ktoré integritné obmedzenia a modely zabezpečenia mobilného operačného systému prelamujú. Dokážu získať plné práva nad procesmi bežiacimi na danom mobilnom zariadení, súborovým systémom, čo v mobilnom zariadení môže byť nežiaduce. Tieto modifikácie často otvárajú dvere novým bezpečnostným problémom, znižujú kompatibilitu a pravdepodobnosť na bezpečnú aktualizáciu na novú verziu mobilného operačného systému daného mobilného telefónu.

3.4.2 Aspekty bezpečnosti

Jednotlivé mobilné operačné systémy spĺňajú kritériá opísané v minulej kapitole na odlišnej úrovni. Niektoré mobilné operačné systémy porovnávané v tejto práci nemajú vyriešené a implementované riešenia na určité bezpečnostné otázky, ako bude ďalej uvedené.

Ochrana heslom

Mobilný operačný systém iOS podporuje základnú ochranu jednoduchým číselným heslom alebo zložitejším alfanumerickým heslom, ktoré užívateľ musí zadať vždy pri zapínaní zariadenia, odomykaní z režimu zamknutej obrazovky. Vymazanie dát po opakovanom chybnom zadaní hesla je taktiež dostupné.

Obdobné možnosti ponúka operačný systém Android, ktorý navyše pridáva možnosť zadávania hesla špecifickým vzorom. Nechýba ani automatické vymazanie dát po chybnom zadaní hesla, každopádne táto možnosť je dostupná až vo verzii Android 2. BlackBerry OS má podporu chránenia heslom rovnako s možnosťou automatického vymazania.

Ochrana SIM karty heslom je samozrejmosťou u všetkých spomenutých mobilných operačných systémoch.

Šifrovanie dát

V otázke šifrovania dát je na tom najlepšie operačný systém iOS, ktorý podporuje šifrovanie dát spolu s jej hardware akceleráciou v prípade zadaného hesla. Nechýba ani zabezpečená virtuálna pamäť.

Podobne je na tom aj BlackBerry OS, ktorý podporuje šifrovanie dát, chránené je aj prípadné externé úložisko dát pre modely BlackBerry telefónov, ktoré nimi disponujú. Výnimkou zo šifrovania môžu byť práve kontakty, ktoré v prípade plného šifrovania pri zamknutom telefóne nekorešpondujú s menami volajúcich, a preto je uvedené iba číslo volajúceho. Preto je dostupná možnosť nešifrovať kontakty.

S podporou šifrovania dát zaostáva mobilný operačný systém Android, ktorý túto podporu má dostupnú až vo verzii Android 3. Aplikácie, ktoré svoje dáta šifrujú kryptografickými algoritmami poskytujú požadovanú ochranu len na úrovni, kam majú prístup. Z toho dôvodu ide momentálne o jediný spôsob ochrany dát šifrovaním, kde pri použití takejto aplikácie na systémoch iOS a BlackBerry OS ide o dvojitú ochranu.

Vzdialené zmazanie dát

Nájdenie mobilného telefónu po jeho stratení či odcudzení primárne podporuje operačný systém iOS ako bezplatnú službu spoločne so vzdialeným vymazaním dát na mobilnom telefóne prípadne jeho uzamknutie. Rovnako na tom je aj mobilný operačný systém Android, ktorý má radu ďalších aplikácií s podobnou funkcionalitou, ale od vývojárov tretích strán. BlackBerry OS ponúka navyše v spojení s BlackBerry Enterprise Server obnovu firemných pravidiel pre zariadenie.

Zálohovanie dát

So vzdialeným vymazávaním dát pri strate či odcudzení mobilného telefónu úzko súvisí záloha týchto dát. Manuálne zálohovanie je veľmi nepraktické a v podnikovej sfére nežiadúce, preto sú potrebné prostriedky pre periodické automatické zálohovanie zariadení.

Najširšie možnosti pre podnikové prostredie v otázke zálohovania dát poskytuje BlackBerry OS. Dokáže zálohovať dáta periodicky spolu s nastaveniami mobilného telefónu. V prípade straty je možné pristúpiť k dátam na diaľku a tak obnoviť dáta, ktoré boli upravené či pridané medzi plánovanými zálohami.

Ostatné nami porovnávané mobilné operačné systémy, dokážu na rozdiel od BlackBerry OS, automaticky iba synchronizovať istý obsah dát ako napríklad kontakty, kalendár, poznámky. V prípade operačného systému Android existujú aplikácie, ktoré napomôžu so zálohovaním. Je potom taktiež možnosť vzdialeného prístupu a zálohy základných údajov, ako napríklad kontaktov.

Mobilný operačný systém iOS v novej verzií iOS 5 dáva vývojárom možnosť zálohy aplikačných dát na serveroch spoločnosti Apple. Rovnako tak môže činiť systém pri pravidelných automatických zálohách, kde zálohuje nastavenia a dáta systémových aplikácií. Potenciálnou výhodou je aj možnosť bezdrôtových rozdielových záloh celého systému po pripojení zariadenia k napájaniu.

Virtuálna privátna sieť

Zamestnanci, ktorí potrebujú pristupovať k firemným informáciám a vnútropodnikovej sieti, musia mať možnosť bezpečného spojenia. Táto najčastejšia potreba podnikovej sféry je v dnešnej dobe implementovaná vo všetkých nami porovnávaných mobilných operačných systémoch. Dostupné sú pokročilé možnosti nastavení certifikátov a autentizácie. BlackBerry OS obmedzuje použitie VPN iba na BlackBerry Enterprise Server.

Riadenie oprávnení

Bezpečnostné politiky jednotlivých podnikov či spoločností sa od seba navzájom môžu líšiť. Tieto politiky a pravidlá spravujú technické oddelenia daných firiem. Možnosti, ktoré týmto oddeleniam mobilné operačné systémy poskytujú, sú rôzne. Či už ide o spôsob nastavovania na diaľku, alebo možnosti, čo všetko na danom mobilnom telefóne je možné sledovať a riadiť.

Pre pokročilé možnosti firemného využitia, riadenia a správy je najznámejší mobilný operačný systém BlackBerry OS. Pomocou BlackBerry Enterprise Server dovoľuje využitie Microsoft Exchange a vlastného spôsobu distribúcie certifikátov a politík bezpečnostných nastavení. Tieto politiky dovoľujú nastaviť, ktoré časti telefónnej výbavy budú používateľovi dostupné, ako napríklad fotoaparát telefónu. Tieto nastavenia pretrvajú aj po prípadnej obnove systému. Každopádne využitie Exchange ActiveSync je možné iba vďaka podpore v aplikáciach tretích strán.

Mobilný operačný systém iOS, ktorý sa v poslednej dobe dostáva do povedomia podnikovej sféry a vzájomného využitia, nepodporuje iOS iba Microsoft Exchange, Exchange ActiveSync ale aj „Vendor Specific Management“ od spoločnosti Cisco. Exchange ActiveSync politiky sú automaticky odosielané na mobilný telefón a celkovo všetky politiky nemôžu byť odinštalované bez administrátorského hesla, alebo je možné definovať, aby nebola možnosť ich odstránenia, pokial nie je telefón kompletne vymazaný. Všetky politiky sú doručené a aktualizované bez nutnosti interakcie používateľa. Tieto zabezpečenia garantujú, že heslá a nastavenia budú správne nastavené podľa smerníc spoločnosti. Konfiguračné profily sú podpísané a šifrované, to umožňuje istotu, že nebudú neoprávnene upravené. Rovnako, ako aj operačný systém BlackBerry OS, iOS umožňuje definovať znemožnenie použitia funkcionalít mobilného telefónu a operačného systému.

Svoju cestu do podnikovej sféry si ešte nezískal operačný systém Android, ktorému vo väčšej miere chýbajú pokročilé politiky a ovládanie funkcií zariadenia. Android svojou novou

verziou operačného systému Android 3 priniesol šifrovanie dát a prináša aj zmeny v politikách a ich širšiu podporu pre väčšie množstvo zariadení. Príkladom sú chýbajúce email politiky pre mnohé zariadenia s mobilným operačným systémom Android. Pre otvorenosť platformy vzniklo mnoho riešení tretích strán, no tie pokročilé vyžadujú zásah do operačného systému a jeho komponentov. Podpora Microsoft Exchange a Exchange ActiveSync je ako natívna tak aj produktmi tretích strán.

Multitasking

Mnoho mobilných operačných systémov je alebo bolo kritizovaných za absenciu podpory multitaskingu, ktorú výrobcovia ospravedlňovali slabou výdržou mobilného zariadenia pri zabudnutí na bežiace aplikácie a spomalenú odozvu grafického rozhrania systému. Niektoré funkcie, chýbajúce v aktuálnych verziách mobilných operačných systémoch, sa snažia vývojári implementovať do svojich aplikácií, no absencia multitaskingu by takúto aplikáciu spravil nepoužiteľnou. Rovnako absencia môže obmedzovať používateľov mobilného zariadenia, ktorí by si priali pracovať efektívnejšie.

Mobilné operačné systémy Android a BlackBerry OS podporujú multitasking bez špeciálnych opatrení vývojárov.

Spoločnosť Apple v aktualizácii svojho mobilného operačného systému na verziu iOS 4 priniesla podporu multitaskingu, ktorá je odlišná od bežnej implementácie. Spočíva v uspaní stavu aplikácie pred vypnutím či prepnutím na inú aplikáciu a v prípade, že daná aplikácia môže vykonávať zmysluplnú činnosť na pozadí, tak vývojári majú prostriedky na implementácie tejto činnosti, ktorá bude vykonávaná aj na pozadí. Táto implementácia by mala šetriť energiu a prostriedky mobilného telefónu.

Riadenie aplikácií

Rozličné bezpečnostné riešenia vývojárskych firiem sú dostupné na platformách Android a BlackBerry OS. Je tomu práve pre možnosti podpísaných aplikácií pristupovať ku dátam iných aplikácií spoločne s rozšírenými možnosťami správy a monitorovania systému z prostredia aplikácie.

V prípade operačného systému iOS, aplikácie bežia v prostredí zvanom „sandbox“. V tomto prostredí aplikácia nemôže pristupovať k dátam iných aplikácií pokiaľ s ňou nezdieľa kľúč. Tento spôsob je pre operačný systém bezpečnejší.

Všetky porovnávané platformy podporujú ochranu pred spustením nepodpísaných aplikácií, avšak v prípade systému Android, je možnosť túto ochranu deaktivovať.

Kapitola 4

Implementácia riešenia

Po vybraní tržne vhodných platforiem z ponuky aktuálne dostupných mobilných operačných systémov na základe analýz kapitoly číslo 2.2 a uvedomení si, čo je možné vyvinúť na týchto platformách s nasledovným zúžením výberu opísaným v kapitole číslo 2.6, sme vybrali pre ďalší vývoj operačné systémy iOS, Android a BlackBerry OS.

Pre významnú profesionálnu penetráciu BlackBerry OS na trhu, má význam vyvinúť aplikáciu, ktorá bude sledovať dianie na mobilných telefónoch, ktoré majú tento systém nainštalovaný. Čím ďalej viac sa rozširujúca platforma Android v radách zamestnancov rôznych spoločností, dáva potenciálny priestor pre aplikáciu, ktorá bude sledovať komunikáciu týchto zariadení s okolitým svetom. V obľube manažmentu sú väčšinou mobilné telefóny spoločnosti Apple s operačným systémom iOS a pre povahu vykonávanej práce je vhodné mať prístup ku nazbieraným dátam od iných zamestnancov, preto vyvinutá aplikácia zobrazuje v prehľadnej forme užívateľovi dáta dostupné na servery. Dôležitý je aj spôsob komunikácie jednotlivých zariadení medzi sebou a miesto pre ukladanie získaných detailných informácií. Tohto účinku je dosiahnuté vyvinutím serverovej aplikácie.

Základom úspešného produktu je aj dôraz na fázu návrhu jednotlivých komponentov, ako aj celého riešenia. Vzhľadom na fakt, že táto kapitola opisuje návrh a vývoj štyroch aplikácií, je nutné pre rovnaké či podobné súčasti zvoliť postup, ktorý bude čo najviac univerzálny a využiť prenositeľné technológie.

V tejto kapitole si priblížime návrh a implementáciu jednotlivých aplikácií ako aj zabezpečenie celého riešenia.

4.1 Spôsoby sledovania dát

Pod pojmom sledovania dát na mobilných telefónoch môžeme rozumieť výklad zaznamenávania komunikácie mobilného telefónu s jeho okolím. Rovnako je možné sledovať dáta aj v mobilnom telefóne a to konkrétne v operačnom systéme ako zaznamenávať pohyb aplikačných dát, multimédií či napríklad geolokačných informácií.

Otázne je ale aké dáta sledovať a akým spôsobom. Mobilné operačné systémy majú prostriedky pre zabezpečenie prístupu k dátam uloženým na mobilnom telefóne, ako je bližšie opísane v kapitole 3.4 na strane 16, na rôznych úrovniach. Veľkým problémom pre rôzne spoločnosti je práve absencia zabezpečenia prenosu a možnosti prístupu k citlivým dátam pri komunikácií mobilného telefónu s jeho okolím. Týmto spôsobom zabezpečenia známe operačné systémy neoperujú.

Žiadne bezpečnostné riešenie nie je dokonalé a vyžaduje celú radu komplexnosti. Preto

záleží na politikách spoločností a úrovni zabezpečenia infraštruktúry, na čo sú dané mobilné telefóny využívané a v akom prostredí. Keďže mobilné telefóny majú možnosť prístupu na internet aj bez využitia firemnej siete a taktiež je ich možné vyniesť tam, kde nie je zamestnanec pod dohľadom je nutné riešiť otázku zabezpečenia prístupu k prenášaným dátam, komunikácie a čo všetko je s mobilom povolené vykonávať.

Potenciálne existujú viaceré spôsoby ako otázku riešiť, ako napríklad vyvinutím hardwarového zariadenia, ktoré sleduje komunikáciu a prípadne ruší neželanú. Takéto riešenie by bolo drahé na vývoj a pravdepodobne komerčne nevyužiteľné pre nepraktickosť. Zabezpečený musí byť daný mobilný telefón či jeho operačný systém. Aby bola komunikácia riadená z čo najnižšej vrstvy, musel by na to byť vybavený daný operačný systém. Možnosťou je preto vyvinúť vlastné riešenie, čo by komerčne nemuselo byť výhodné.

Výhodnejšia varianta je použiť existujúci operačný systém s možnosťou licencovania a úprav, ako napríklad Android. Takéto riešenie by mohlo byť ďalej ponúkané klientom a inštalované na škálu zariadení, ktoré tento operačný systém podporujú. Komplexnosť riešenia by bola výzvou pre bezpečnostné spoločnosti, pre nutnosť úprav operačného systému od jeho jadra, sieťovej vrstvy, súborového systému, správy administrácie, šifrovania a aktualizácií systému.

Alternatívou k tomuto riešeniu je využitie skutočnosti už existujúcich inštalácií mobilných operačných systémov na telefónoch, dodatočným zabezpečením systému. Takéto riešenie si vyžaduje možnosť prístupu na všetky vrstvy operačného systému, konkrétne by to vyžadovalo vykonať proces zvaný „rooting“ u Androidu a „jailbreak“ na platforme iOS. Tým by sa musela riešiť otázka zákonnej záručnej lehoty, pretože tento postup väčšinou porušuje záručné podmienky spoločnosti.

Riešením, ktoré nevyžaduje žiaden zásah do mobilných operačných systémov je vyvinutie aplikácie, ktorá bude komunikovať s operačným systémom pomocou dostupných metód a rozhraní. Tento prístup má svoje limity a to vo forme obmedzení daných SDK, ktoré je nutné rešpektovať. Nie každý operačný systém otvorene disponuje takýmito metódami a preto sa jednotlivé bezpečnostné riešenia od seba líšia a prakticky nie je preto možné nízkoúrovňové sledovanie a riadenie toku dát.

Prvým krokom je komunikáciu sledovať. Preto jednotlivé aplikácie budú zaznamenávať SMS komunikáciu, históriu telefonátov a emailovú komunikáciu.

4.2 Databáza

Pre nutnosť ukladať detailné informácie o zaznamenaných udalostiach v jednotlivých aplikáciách a na servery je vhodné využiť relačnú databázu SQLite, ktorá je dostupná[1] na všetkých využitých platformách.

Jednotlivé aplikácie sa od seba čo sa týka návrhu databáze odlišujú, každopádne základ je rovnaký a je uvedený na obrázku číslo 4.1. Aplikácie na mobilnom operačnom systéme Android a BlackBerry OS rozširujú toto schéma o nový stĺpec a to `sent`, ktorý označuje, či bol daný záznam úspešne odoslaný na vzdialený server.

Na druhú stranu, návrh databázy na platforme iOS z dôvodu toho, že táto aplikácia slúži na zobrazenie nazbieraných záznamov z iných mobilných telefónov, tak rozširuje základné schéma o stĺpec `UID`, udávajúci z akého mobilného telefónu pochádza. Taktiež pridáva novú tabuľku s názvom `version` a stĺpcami `number` a `database`.

[1] Prehľadný popis nasadenia je dostupný na adrese http://sqlite.org/mostdeployed.html

Sú tu uchované informácie ako verzia databázy a aktuálnych záznamov, ktoré iOS aplikácia zo serveru získala. Týmto spôsobom je zaručené korektné verziovanie a vďaka tomu nie sú prenášané nadbytočné dáta.

Návrh databázy serverovej aplikácie rozširuje iOS návrh a pridáva tabuľku `users` so stĺpcami `_id`, `login`, `password` a `hash`, v ktorých sú uložené informácie o užívateľoch, aby bola možná autentizácia.

Spôsob zabezpečenia jednotlivých databáz alebo ich položiek, je bližšie rozvedený v kapitole 4.6.

Obr. 4.1: Základný databázový model

4.3 Objektový návrh

S využitím návrhových vzorov [8] pri návrhu aplikácií, je možné elegantne riešiť niektoré problémy a vyrobiť znovu použiteľné riešenie. Počas návrhu mobilných aplikácií boli použité vzory `Singleton`, `Observer` a okrem aplikácie pre BlackBerry OS aj `Model view controller`.

4.3.1 Android

S využitím implementačného jazyku Java je možné mať viac vstupných bodov do aplikácie a to pomocou konfigurácie v súbore `AndroidManifest.xml`. Aplikácia je vyvinutá pre Android 2.3.3 s API úrovňou 10 a jej názov je `AndroidWatcher`.

Má dve aktivity, a to zobrazenie aplikácie a uložených záznamov, o čo sa stará trieda `AndroidWatcherActivity` spoločne s aktivitou zobrazenia nastavení, ktoré sú v správe triedy `Preferences`. Aplikácia zaznamenáva komunikáciu pomocou volaní a SMS, o čo sa starajú triedy `CallReceiver` a `SMShandler`. Aplikácia musí mať užívateľom potvrdené oprávnenia, aby mohla korektne naslúchať, toto potvrdenie je zadané pri inštalácii aplikácie.

Jednotlivé záznamy sú uložené do databázy pomocou triedy `dbHelper`. Zasielanie záznamov na vzdialený server je v réžii triedy `Networker`, ktorá taktiež implementuje zabezpečenie SSL. Pre podporu vlastnoručne podpísaných certifikátov sú vytvorené triedy `EasySSLSocketFactory` a `EasyX509TrustManager`, ktoré dokážu takýto certifikát prijať. Aby bolo možné sledovať stav internetu a pri zapnutí automaticky preposlať neodoslané záznamy slúži trieda `NetworkReceiver`.

4.3.2 iOS

Aplikácia s názvom `PhoneLogs` je implementovaná v jazyku Objective – C verzie 2.0, pre mobilný operačný systém iOS 5.1.

Vstupným bodom je trieda `AppDelegate`, ktorá zinicializuje chod aplikácie. O zobrazenie záznamov v kategóriách sa stará trieda `UniversalTableView`, ktorá je základom pre štyri ďalšie triedy, ktoré z nej dedia a nastavujú čo sa má zobraziť. Obsah zobrazenej plochy je uložený v databáze, nad ktorou operácie spravuje trieda `Database` s využitím FMDB knižnice[2].

Detaily o uloženom zázname su zobrazené pomocou `DetailsViewController` a prijaté vďaka úkonom triedy `Connection` vrátane implementácie bezpečného spojenia SSL. Objekt reprezentujúci záznam je reprezentovaný inštanciou triedy `Log`. Animované zobrazenie načítania pri čakaní na dokončenie sieťovej operácie rieši `LoadingView`.

4.3.3 BlackBerry OS

Pre SDK verzie 7.1 bola vyvinutá aplikácia s názvom `BlackBerryWatcher`, ktorá ako jediná z mobilných aplikácií nie je navrhnutá so zreteľom na návrhový vzor `Model view controller`. Pre rozdiely medzi SDK systému Android a BlackBerry OS sú jednotlivé triedy implementačne odlišné.

Vstupným bodom je implementácia triedy `MyApp` so zobrazením `MyScreen`. Rovnako ako Android aplikácia tak aj táto zaznamenáva komunikáciu pomocou volaní a SMS, konkrétne pomocou `CallLogger` a `SMSLogger`. Pridáva taktiež možnosť sledovania mailovej komunikácie pomocou triedy `MailLogger`.

Na rozdiel od Android implementácie, neposkytuje možnosť detekcie pripojenia internetu, poskytuje ale zistenie odpojenia a pripojenia externého úložiska vo forme SD karty, ktorá je kľúčová pre chod aplikácie pomocou `cardListener`. Ukladanie do databázy je možné vďaka `dbHelper`. Správu užívateľských výziev zabezpečuje `CustomDialog` a formátovanie dátumu rieši statická trieda `CustomDateFormatter`.

Zasielanie jednotlivých záznamov na vzdialený server s podporou SSL implementuje trieda `Networker`. Perzistentné uloženie užívateľských nastavení je dosiahnuté v triede `Settings`.

4.3.4 Server

Pre prenositeľnosť implementácie serveru, bol zvolený jazyk Python verzie 2.7. Aj keď je vo veľkej miere nasadzovaná verzia Python 3 a jej výhody verejne diskutované[3], dostupnosť kryptografických knižníc pod touto verziou je nedostačujúca.

Serverová aplikácia sa skladá z viacero modulov, ako analýza parametrov `parameters`, či overenie prerekvizít pomocou `prereq`, aby aj v prípade chýbajúcich knižníc pre jednu z dôležitých funkcionalít administrátor vedel, čo je treba doinštalovať. Vynášanie a obsluha výnimiek je dosiahnutá vlastnou implementáciou v module `myerror`.

Prácu s databázou a všetky požadované operácie nad ňou zabezpečuje modul `database`, ktorý úzko komunikuje s modulom `crypter`, majúci na starosti pokročilé šifrovanie položiek ukladaných do databázy. Tieto záznamy sú buď čítané pre účel zaslania do iOS PhoneLogs aplikácie alebo na povel implementácie serveru, sú zapísané po prijatí z aplikácií AndroidWatcher alebo BlackBerryWatcher.

[2] Knižnica stiahnuteľná zo stránky https://github.com/ccgus/fmdb

[3] Článok je dostupný na adrese http://wiki.python.org/moin/Python2orPython3

Beh aplikácie riadi serverová časť, teda modul `server`, ktorá dokáže obsluhovať viacero požiadavok súčasne[4]. Server komunikuje s mobilnými aplikáciami pomocou POST HTTP[5] dotazov, prípadne so SSL zabezpečením. Po prijatí takejto požiadavky, ho analyzuje pomocou modulu `analyse` a podľa požadovanej činnosti vykoná obsluhu, modulom `coder` vytvorí odpoveď a následne ju odošle. Prítomný je aj modul `manager`, ktorý má na starosti správu užívateľov.

4.4 Formát posielaných dát

Serverová aplikácia je stredom diania, ukladá prijaté záznamy z aplikácií AndroidWatcher a BlackBerryWatcher a poskytuje ich autentizovaným užívateľom napríklad prostredníctvom PhoneLogs aplikácie.

Komunikácia je pomocou HTTP POST požiadaviek, prípadne v zabezpečenej HTTPS[6] forme. Preposielané dáta a požiadavky sú v JSON[7] objektovej notácií. V kóde číslo 1 je možno vidieť štruktúru odpovede, zasielanej zo serveru aplikácií PhoneLogs. Vďaka verziovaniu databázy, je možné zasielať iba tie záznamy, ktoré aplikácia ešte nedostala. Týmto spôsobom je možné riadiť požadované správanie prijímacej strany, ako detekcia odhláseného užívateľa či požiadavok na zmazanie databázy.

Pokiaľ neprenesených záznamov je viac, sú zaslané v celku a sú dostupné v poli. Formát položky v poli je rovnaký ako aj zasielaný JSON objekt zo zberných aplikácií. Dotazy na server a autentizačné správy sú taktiež v tomto formáte.

```
{
  "database":2,
  "version":2,
  "dump":"false",
  "validity":"true",
  "records":
   [ {
      "body":"text",
      "fromNumber":"111",
      "toNumber":"15555215554",
      "UID":"15555215554",
      "service":"SMS",
      "date":"27.04.2012",
      "device":"Android",
      "time":"21:58",
      "typeMessage":"IN"
   } ]
}
```

Kód 1: Ukážka prenášaného JSON objektu

[4] Limitujúc možnosťou vytvárania nových procesov
[5] Hypertext Transfer Protocol
[6] Hypertext Transfer Protocol Secure
[7] JavaScript Object Notation

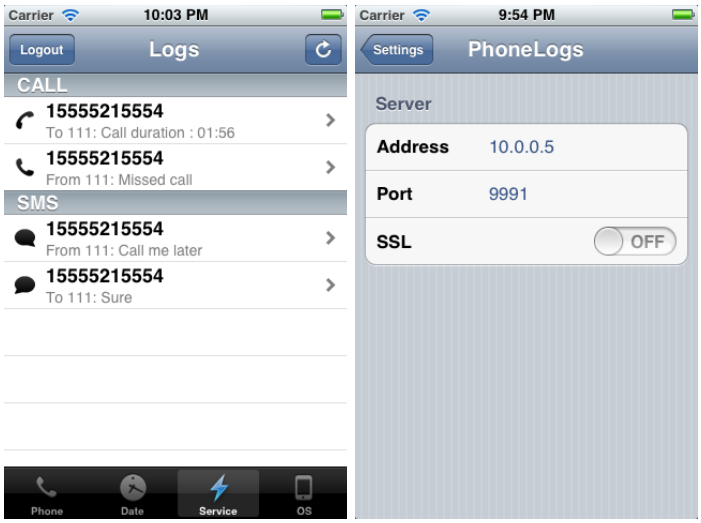
4.5 Užívateľské rozhranie

Všetky tri mobilné aplikácie dokážu užívateľovi zobraziť zachytené záznamy a taktiež poskytujú možnosť nastaviť adresu vzdialeného serveru a preferenciu použitia SSL. Rozhrania pre užívateľskú prívetivosť boli navrhnuté pomocou odporúčaní jednotlivých spoločností.

4.5.1 iOS

Aplikácia PhoneLogs zobrazená na obrázku číslo 4.2 rešpektuje odporúčania spoločnosti Apple [2]. Rozhranie poskytuje štyri záložky, v ktorých je filtrovo závislé zobrazenie záznamov. Tieto položky sú zobrazené a radené do zoznamu a po prejdení prstom sú zobrazené jeho detaily. Pre lepšiu orientáciu medzi položkami sú použité rôzne ikony zobrazujúce typ záznamu a smer komunikácie.

Prihlásenie užívateľa pre jeho autentizáciu je riešené vyzývacím dialógom a všetky operácie, ktoré trvajú dlhší čas ako napríklad načítanie nových záznamov, zobrazujú užívateľovi čakací dialóg. Nastavenia detailov pre spojenie so serverom, je umiestnené do nastavení iOS sekcie aplikácie tretích strán, tak ako to spoločnosť odporúča.

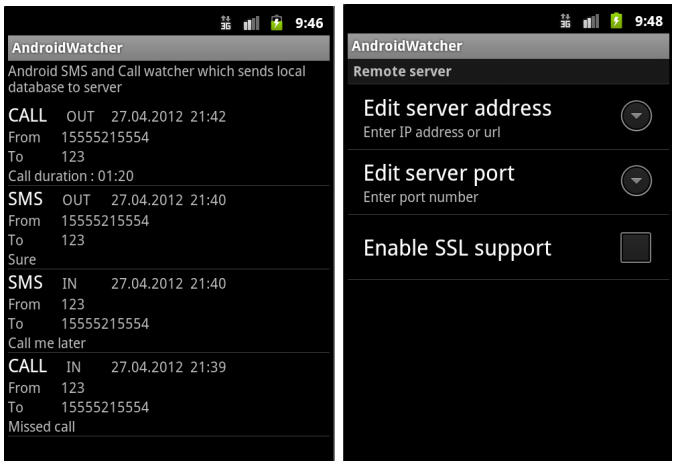


Obr. 4.2: Užívateľské rozhranie aplikácie PhoneLogs

4.5.2 Android

Na druhú stranu, mobilná aplikácia AndroidWatcher zobrazuje zachytené záznamy, dostupné na danom telefóne. Na rozdiel od PhoneLogs, ako je vidieť na obrázku číslo 4.3, aplikácia zobrazuje detailné informácie o uloženom zázname už v zozname položiek.

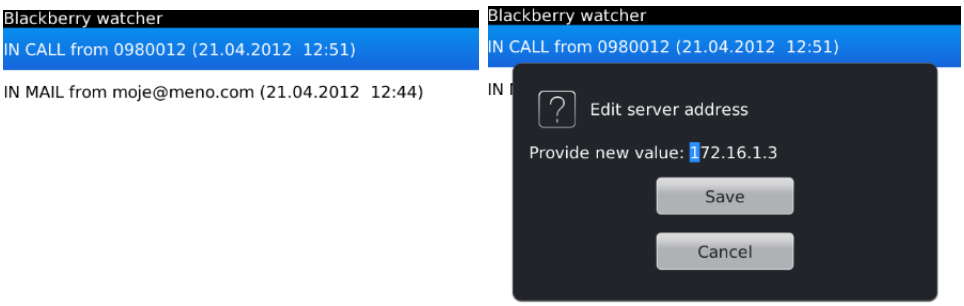
Pre univerzálnosť návrhu rozhrania bolo nutné postupovať podľa odporúčaní spoločnosti Google [13]. Táto skutočnosť sa prejavila aj pri návrhu nastavení, ktoré na rozdiel od iOS aplikácie sú súčasťou aplikácie. Rovnako aj táto aplikácia zobrazuje čakací dialóg pri preposielaní či pripájaní na vzdialený server.



Obr. 4.3: Užívateľské rozhranie aplikácie AndroidWatcher

4.5.3 BlackBerry OS

Aplikácia BlackBerryWatcher navrhnutá podľa odporúčaní spoločnosti RIM [17], vyžaduje jednoduchosť na prvom mieste. Je toho dosiahnuté zobrazením zoznamu zachytených záznamov vo forme jednoriadkového formátovaného textu, ako je tomu na obrázku číslo 4.4. Nastavenia sú riešené zobrazením vyzývacieho dialógu a čakací dialog je taktiež dostupný.



Obr. 4.4: Užívateľské rozhranie aplikácie BlackBerryWatcher

4.6 Zabezpečenie

Z dôvodu povahy prenášaných dát, kde ide o interné informácie ako emailová komunikácia, či obsah SMS, je nutné riešiť otázku ochrany dát. Neoprávnená osoba by nemala mať vzdialený prístup k dátam uloženým na serveri, taktiež ani v prípade získania lokálnej databázy. Nemala by byť ani schopná odpočúvať komunikáciu medzi mobilnými aplikáciami a serverom.

4.6.1 Databáza

Nie každý mobilný operačný systém, ako je opísané v kapitole číslo 3.4.2 poskytuje šifrovanie súborového systému. Preto využitím symetrickej kryptografie v podobe použitia knižnice SQLCipher[8] je možné jednotlivé databázy zabezpečiť. Je tomu tak pri aplikácií AndroidWatcher, pretože operačný systém Android v použitej verzii neposkytuje šifrovanie súborového systému. Aplikácia PhoneLogs pre platformu iOS využíva spomenutú knižnicu, každopádne ide o dvojitú ochranu, keďže jej súborový systém podporuje šifrovanie. Knižnica SQLCipher zabezpečuje databázu symetrickou šifrou s algoritmom AES v móde CBC, ako je bližšie vysvetlené v kapitole 3.1.1 na strane 12. Kľuč je 256 bitový a inicializačné vektory sú pre každý záznam pseudo náhodne vygenerované.

Vzhľadom na to, že knižnica pracuje po stránkach, tak nevyžaduje načítanie celej databázy. Výhodou operačného systému BlackBerry OS je fakt, že podporuje šifrovanie SQLite databázy bez potrebného použitia knižnice tretích strán. Rovnako ako SQLCipher, aj BlackBerryWatcher databázu šifruje 256 bitovým kľúčom AES symetrickej šifry. Limitom implementácie šifrovania v podaní tohto operačného systému je neprenositelnosť databázy v zašifrovanej podobe na iný mobilný telefón ako zdrojový.

Priorita zabezpečenia databázy v prípade serverovej implementácie je vysoká a to aj pre dôvod združovania všetkých dostupných záznamov. Položky databáze sú preto zašifrované symetrickou šifrou algoritmom AES v CBC móde a inicializačné vektory sú vždy pseudo náhodne vygenerované. Rozšírením bezpečnosti je generovanie AES kľúča pre každý záznam v databáze vždy pseudo náhodne. AES šifrovanie je slabé pokiaľ je s jedným kľúčom zašifrovaných veľké množstvo záznamov a vždy je použitý rovnaký inicializačný vektor. Vzhľadom na fakt, že takáto kombinácia v implementácií serveru nastane s malou pravdepodobnosťou, znižujeme bezpečnostné riziko, keďže ako kľuč tak aj inicializačné vektory sú generované.

Tento kľúč je zašifrovaný asymetrickou šifrou v podobe algoritmu RSA, opísanom v kapitole 3.1.2, rozšíreným o štandard PKCS #1, využitím 1024 bitového kľúča. V prípade vytvárania novej databázy je privátny kľúč vyexportovaný v podobe certifikátu, ktorý môže byť uložený v zašifrovanej podobe, kde kľúč šifry je odvodený od zadaného hesla. Tento certifikát je ďalej využívaný a importovaný v prípade reštartu serveru. Jadro kryptografických operácií ako implementáciu jednotlivých šifrovacích algoritmov zabezpečuje Python knižnica PyCrypto[9].

[8] Zabezpečenie je stiahnuteľné z adresy http://sqlcipher.net/
[9] Knižnica je dostupná na adrese https://www.dlitz.net/software/pycrypto/

4.6.2 Komunikácia

Vzhľadom na to, že dáta sú prenášané v textovej podobe v podobe JSON, opísanom v kapitole 4.4, zabezpečenie jednotlivých databáz a nezabezpečenie prenosu dát medzi nimi by bolo nebezpečné. Komunikácia prebieha pomocou HTTP protokolu využitím jednej z dotazovacích metód a to metódy POST. Aby bolo spojenie medzi mobilným telefónom a vzdialeným serverom zabezpečené, je vytvorené SSL spojenie opísané v kapitole 3.2.

Spojenie je potom šifrované a komunikujúce strany sa navzájom autentizovali. Pre využitie zabezpečeného spojenia je nutné aplikácii dodať certifikát, ktorý je možné získať od certifikačných autorít alebo vygenerovať príkazom, ktorý je uvedený v kóde číslo 2.

```
openssl req -new -x509 -keyout cert_server.pem \
-out cert_server.pem -days 365 -nodes
```

Kód 2: Príkaz pre vygenerovanie SSL certifikátu

4.6.3 Autentizácia

Aby server neposkytoval uložené záznamy komukoľvek, má databázu užívateľov, ktorý majú prístup k týmto dátam a preto je nutné sa autentizovať. Autentizácia prebieha porovnaním užívateľského mena a hesla v podobe SHA256 otisku, ktorý je opísaný v kapitole 3.1.4 na strane 13. Pokiaľ zadaný užívateľ existuje, je aplikácií vrátený identifikátor relácie, ktorú bude používať pri požiadavkách o získanie dát.

Aplikácia PhoneLogs implementuje proces získania týchto údajov, zaslanie na vzdialený server a následné komunikovanie v podobe predávania identifikátoru relácie.

Kapitola 5

Vyhodnotenie funkcionality

Jednotlivé aplikácie slúžia na rôzne účely a tomu zodpovedá aj ich požadovaná a nasledovne implementovaná funkcionalita. Štyri vyvinuté aplikácie sú rozdelené do troch skupín a to do kategórie zberu jednotlivých záznamov, zobrazenia všetkých dostupných záznamov a serverovej aplikácie, ktorá zabezpečuje vzájomnú centralizovanú komunikáciu.

5.1 Zber záznamov

Aplikácie AndroidWatcher a BlackBerryWatcher pre svoje SDK umožňujú zbieranie záznamov o komunikácii mobilného telefónu s jeho okolím. Konkrétne AndroidWatcher dokáže zachytiť prichádzajúce a odchádzajúce SMS správy ako aj volania. Aplikácia pracuje na pozadí a dokáže detekovať zmeny stavu pripojenia na internet.

V prípade nemožnosti odoslať jednotlivé záznamy na vzdialený server, pokúsi sa akciu opakovať neskôr, alebo ich automaticky prepošle pri znovapripojení na sieť internet za predpokladu, že je server spustený a sú korektne nastavené detaily spojenia aplikácie so serverom. Pri zmene nastavení je užívateľ informovaný o úspešnosti pripojenia na server s novými údajmi. Na pozadí aplikácie sú stále zobrazené zaznamenané položky aj s ich detailmi. V prípade, že užívateľovi prekážajú, je možné ich z vymazať výberom operácie z kontextového menu.

Najprv sa ale skontroluje, či záznamy už boli odoslané, pokiaľ tomu tak nie je, sú najprv odoslané a možnosť ich vymazania je až po ich úspešnom odoslaní. Pre lepšiu prehľadnosť je užívateľ informovaný čakacím dialógom, aby mal predstavu, že sa záznamy preposielajú na vzdialený server. V nastaveniach je taktiež možné zmeniť preferenciu bezpečného spojenia so serverom. Ukážku užívateľského rozhrania je možné vidieť na obrázku 4.3 na strane 27.

Rovnaké funkcionality má aj aplikácia BlackBerryWatcher, ktorá pridáva podporu zaznamenávania emailovej komunikácie. Neposkytuje možnosť detekcie zmien stavu pripojenia k internetu, ale pridáva podporu detekcie pridania či odobrania externého úložiska. Databáza totiž musí byť na ňom uložená a to pre univerzálnosť a kompatibilitu s celou škálou BlackBerry zariadení. Na obrázku 4.4 je vidieť užívateľské rozhranie v prevedení operačného systému BlackBerry OS.

5.2 Zobrazenie záznamov

Zobraziť vlastné záznamy dokážu aplikácie AndroidWatcher a BlackBerryWatcher, každopádne zobraziť všetky dostupné záznamy načítané zo vzdialeného serveru umožňuje aplikácia PhoneLogs. Po vyzvaní užívateľa pre získanie platného prihlasovacieho mena a hesla začne komunikovať so serverom. Aplikácia si udržuje číslo databázy a verziu záznamov, ktoré spoločne s požiadavkou o získanie dát a identifikátorom relácie zasiela serveru.

Ten jej poskytne aktuálne dáta, každopádne vďaka použitému verziovaniu minimalizuje veľkosť prenášaných dát iba na zatiaľ neprenesené záznamy. Jednotlivé záznamy sú zobrazené vo forme zoznamu a v prípade výberu jednej z položky sú zobrazené jej detaily. Radenie jednotlivých záznamov závisí od vybranej kategórie, kde na výber sa ponúka zobrazenie podľa zariadenia, dátumu, typu záznamu a operačného systému. Ukážku je možné vidieť na obrázku číslo 4.2 na strane 26.

Prívetivosť je doplnená o zobrazenie čakacieho dialógu pri potenciálne zdĺhavom načítavaní dát zo serveru. Aplikácia taktiež detekuje, či vzdialený server beží s podporou SSL spojenia, alebo nie. Rieši tak prípadnú kolíziu preferencií v nastaveniach a dáva možnosť používateľovi priamej nápravy.

5.3 Server

Implementácia serverovej aplikácie musí podporovať reakcie na potenciálne súbežné požiadavky jednotlivých mobilných aplikácií. Súčasťou sú aj zistenia validity jednotlivých požiadavok ako aj kontroly či sú autorizované na požadovanú činnosť. Potrebná je aj správa užívateľov a práca s databázou, ktorá vyžaduje vytvorenie certifikátu pre podpis položiek v databáze rovnako ako aj overenia, či daný certifikát alebo celá databáza nie je podvrhnutá.

Administrátor je upozornený aj na zmeny certifikátu, pokiaľ už nejaké položky existujú a boli podpísané iným certifikátom, pretože by nebolo možné ku existujúcim pristupovať. Server taktiež podporuje zmazanie databázy záznamov, bez toho aby bolo nutné zmazať databázový súbor, stratili by sa tak totiž záznamy o užívateľoch. Pre bezpečné spojenie pomocou SSL, je nutné poskytnúť serveru certifikát, ktorého validitu si aplikácia overí.

Server je možné spustiť na ľubovoľnom voľnom porte, alebo si ho vyberie automaticky sám. Pre výpomoc administrátorovi s inštaláciou prípadných knižníc, implementácia serveru si zistí, ktoré knižnice chýbajú a v prípade, že by nebolo možné spustiť aplikáciu, poskytne túto informáciu. Manuál akým spôsobom pracovať so serverovou aplikáciou a zoznam možných prepínačov je dostupný v prílohe A na strane 36.

5.4 Použitie aplikácií

V prípade rozhodnutia sa využiť bezpečnostné riešenie tejto práce, je možné po skompilovaní jednotlivých aplikácií, ich nainštalovať na mobilných telefónoch. AndroidWatcher bude nasledovne zaznamenávať SMS správy spoločne s históriou hovorov a BlackBerrryWatcher k tomu ešte pridá sledovanie emailovej komunikácie. Po správnom nakonfigurovaní serverovej aplikácie a nastavení mobilných aplikácií, bude prebiehať komunikácia medzi zariadeniami a serverom a to podľa preferencií aj v zabezpečenej forme SSL spojenia. Manažérska aplikácia PhoneLogs pre platformu iOS po úspešnej autentizácií zobrazí všetky dostupné záznamy, načítané zo vzdialeného serveru.

Ukážkovou komunikáciou medzi dvoma zariadeniami, kde jedna strana má nainštalovanú

aplikáciu AndroidWatcher, je demonštrovaná funkčnosť vyvinutého riešenia. Ako je vidieť na obrázku číslo 4.3 na strane 27, komunikácia začína neprijatým hovorom. Nasleduje SMS správa, ktorá inštruuje adresáta aby keď bude dostupný, zavolal na telefónne číslo späť. Príjemca tejto správy potvrdí porozumenie svojou odpoveďou. Za okamih vykoná prisľúbený telefonát, ktorý druhá strana prijme.

Zaznamenané informácie sú prehľadne a detailne zobrazené na pozadí aplikácie a v okamihu ich zaznamenania sú zaslané na vzdialený server. Poverená osoba má možnosť si ich zobraziť na svojom iOS zariadení v aplikácií PhoneLogs. Po úspešnej autentizácii sú dáta načítané zo serveru a zobrazené ako je tomu vidieť na obrázku 4.2. Prehľadne sú zobrazené informácie ako z akého mobilného telefónu je daný záznam, typ komunikačného prostriedku ako aj smer komunikácie.

Medzi neodmysliteľné výhody vyvinutého riešenia patrí jednoduchosť jej nasadenia a minimálnej potreby konfigurácie, ktorá je bližšie opísaná v prílohe A. Aplikácie pracujú na pozadí a nie je potrebná ich dodatočná obsluha a vďaka zabezpečeniu opísanom v kapitole číslo 4.6, by sa malo riešenie a jednotlivé aplikácie dať použiť aj v podnikovej sfére. Výhodou je taktiež rešpektovanie odporúčaní pri vývoji grafického užívateľského rozhrania pre lepšiu integráciu aplikácie do povedomia používateľov daného operačného systému.

Vzhľadom na limitujúce prostriedky prístupu k regulačným funkciám mobilných operačných systémoch, ktoré v jednotlivých SDK nie sú dostupné, riešenie nedokáže dynamicky reagovať a neželanej komunikácií zabrániť. Kapitola číslo 3.4 o tomto probléme pojednáva.

5.5 Testovanie

Pri vývoji mobilných aplikácií sú dve možnosti na ladenie, a to využitím dostupných nástrojov, ktoré emulujú mobilné operačné systémy mimo mobilné zariadenia ako je opísané v kapitole 2.5.4 na strane 10, alebo ladenie na reálnych zariadeniach. Väčšina platforiem vyžaduje zakúpené licencie, aby bolo možné aplikáciu na mobilný telefón nainštalovať. Ceny licencií sú popísané v kapitole 2.5.2.

Preto boli aplikácie testované iba v emulátoroch svojich mobilných operačných systémov. Počas vývoja boli otestované a ladené jednotlivé moduly, celé aplikácie ako aj komplexné riešenie. Serverová aplikácia korektne deteguje podvrhnutú databázu či certifikáty, rovnako aj chýbajúce moduly či knižnice. Pre otestovanie správneho zaznamenávania SMS správ boli emulátory medzi sebou prepojené. Taktiež bol spustený BES[1] a email server, pre otestovanie korektného zaznamenávania emailovej komunikácie.

Aby neboli limitujúci užívatelia komunikujúci v iných znakových sadách ako latinka, úspešne boli napríklad zaznamenané, odoslané a zobrazené čínske znaky. Taktiež nie je problém vytvorenia užívateľa s prihlasovacím menom či heslom obsahujúcim diakritiku.

[1] BlackBerry Enterprise Server

Kapitola 6

Záver

Hlavným výstupom spracovania tejto práce je komplexné bezpečnostné riešenie, ktoré poskytuje možnosť sledovať komunikáciu mobilných telefónov s ich okolím. Návrhu predchádzala analýza trhu mobilných operačných systémov, na ktoré malo byť riešenie vyvinuté. Po zistení penetrácie jednotlivých platforiem a odhadu trendov bol výber zúžený na systémy Android, BlackBerry OS, iOS, Symbian a Windows Phone.

Významnosť bezpečnostných riešení v mobilných platformách je možné priblížiť vďaka opisu vyjadrení a spracovaním súhrnov názorov spoločností na problematiku. Vďaka spracovanej technickej analýze a porovnaní jednotlivých mobilných operačných platforiem z pohľadu vývoja a testovania, ako aj licenčných podmienok, boli pre vývoj bezpečnostného riešenia vybrané najvýhodnejšie platformy. Rovnako aj pohľad na bezpečnostné možnosti a zhodnotenie kritérií zavážili pri výbere systémov Android, BlackBerry OS a iOS.

Na tieto platformy bolo vyvinuté riešenie pre sledovanie dát na mobilných telefónoch formou zaznamenávania komunikácie. To pozostáva z aplikácie AndroidWatcher, ktorá zaznamenáva SMS správy, históriu volaní a aplikácia BlackBerryWatcher k tomu pridáva emailovú komunikáciu. Záznamy sú zasielané a zhromažďované na serverovej aplikácii, ktorá taktiež obsahuje správu užívateľov pre autentizáciu. Pomocou mobilnej aplikácie PhoneLogs, dostupnej na platforme iOS, si je možné prehľadne zobraziť záznamy dostupné na vzdialenom serveri.

Pre povahu ukladaných a posielaných dát, je nutnosť zabezpečiť jednotlivé úložiska šifrovaním. Možnosť neoprávneného prístupu k dátam uloženom na servery dáva priestor pre zavedenie užívateľskej autentizácie. Riziko odpočúvania komunikácie mobilných aplikácií so vzdialeným serverom je znížené použitím zabezpečenia spojenia SSL certifikátom. S komplexnosťou vyvinutého riešenia prichádza potenciál pre uplatnenie v praxi obohatené ukázaním možností rozšírení pre komerčné využitie.

Vzhľadom na čoraz väčší počet mobilných zariadení Android u zamestnancov manažérskych pozícií, by bolo žiadaným rozšírením pre aplikácie AndroidWatcher a BlackBerryWatcher, podpora zobrazenia záznamov uložených na vzdialenom serveri.

Dokým SDK jednotlivých mobilných operačných systémov nebudú podporovať regulačné mechanizmy pre potrebu riadenia neželanej komunikácie, rozšírenie v podobe informovania administrátora alebo inej povolanej osoby v prípade detekcie takejto komunikácie, je v podnikovej sfére želané. V závislostí od nastavených politík spoločností by mohla byť vyžadovaná podpora sledovania komunikácie v podobe MMS správ.

Literatúra

[1] *The 2010 U.S. Digital Year in Review*. Reston, VA, USA: comScore, Inc, 2011.

[2] Bondo, J. *iPhone User Interface Design Projects*. Berkely: Apress, 1st edition, 2009. ISBN 1-430-22359-6.

[3] Constantinou, A. *Developer Economics 2011* [online]. c2005 – 2011, [cit. 2011-06-22]. URL http://visionmobile.com/devecon.php

[4] Coutinho, S. *The mathematics of ciphers: number theory and RSA cryptography*. London: A K Peters, 1999. ISBN 1-568-81082-2.

[5] Daemen, J.; Rijmen, V. *The Design of RijndaeL: AES - The Advanced Encryption Standard*. Berlin: Springer-Verlag, 2002. ISBN 3-540-42580-2.

[6] Ferguson, N.; Schneier, B.; Kohno, T. *Cryptography Engineering: Design Principles and Practical Applications*. Minneapolis: John Wiley & Sons, 2010. ISBN 2-010-92064-8.

[7] Fisher, D. *Enterprise Mobile Security Survey* [online]. c2011, [cit. 2011-06-14]. URL http://threatpost.com/enterprise-mobile-security-survey-results

[8] Fowler, M. *Patterns of Enterprise Application Architecture*. Massachusetts: Addison-Wesley Professional, 2002. ISBN 0-321-12742-0.

[9] Hildahl, B. *Survey of Fortune 500 companies reveals plans to invest in mobile offerings* [online]. c2011, [cit. 2011-06-20]. URL http://kony.com/marketing/mobile_report/

[10] Housley, R.; Polk, W.; Ford, W.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, April 2002. URL http://www.ietf.org/rfc/rfc3280.txt

[11] Jonsson, J.; Kaliski, B.: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography. RFC 3447, February 2003. URL http://www.ietf.org/rfc/rfc3447.txt

[12] Kaliski, B.: PKCS #7: Cryptographic Message Syntax. RFC 2315, March 1998. URL http://www.ietf.org/rfc/rfc2315.txt

[13] Morris, J. *Android User Interface Development: Beginner's Guide*. Birmingham: Packt Publishing, 2011. ISBN 1-849-51448-8.

[14] Oltsik, J. *Addressing Mobile Device Security and Management Requirements in the Enterprise* [online]. c1999 – 2011, [cit. 2011-06-15].
URL http://juniper.net/uk/en/dm/mobile-security

[15] Pettey, C. *Market Share Analysis: Mobile Devices, Worldwide, 1Q11* [online]. c2011, [cit. 2011-06-20].
URL http://gartner.com/it/page.jsp?id=1689814

[16] Restivo, K. *Global smartphone market expected to grow 55 % in 2011* [online]. c2011, [cit. 2011-06-20].
URL http://idc.com/getdoc.jsp?containerId=prUS22871611

[17] Rizk, A. *Beginning BlackBerry Development*. New York: Apress, 2009. ISBN 2-011-29363-0.

[18] Shah, H. *AdMob Publisher Survey* [online]. c2005 – 2009, [cit. 2011-06-22].
URL http://metrics.admob.com/2010/03/admob-publisher-survey/

[19] Singh, A. *Mac OS X Internals: A Systems Approach*. 1st edition. Massachusetts: Addison-Wesley Professional, 2006. ISBN 0-321-27854-2.

[20] Slavík, P. *Laboratorní úloha infrastruktury veřejných klíčů*. Diplomová práce, FEEC VUT v Brně, 2009.

[21] Tewari, N. *A Global Consumer View of Mobile Advertising* [online]. c2008 – 2011, [cit. 2011-06-15].
URL http://www.inmobi.com/consumer-research

Dodatok A

Manuál

Pre sfunkčnenie vyvinutého riešenia je nutné mobilné aplikácie najprv preložiť do podoby, inštalovateľnej do mobilných telefónov alebo emulátorov platforiem. Pre inštaláciu na mobilné telefóny je potrebné aplikácie podpísať zakúpenou licenciou.

Aplikácie AndroidWatcher a BlackBerryWatcher je možné priamo skompilovať z prostredia Eclipse za predpokladu nainštalovaných SDK balíčkov. AndroidWatcher vyžaduje Android 2.3.3 a BlackBerryWatcher zas SDK BlackBerry OS verzie 7.1.

Na druhú stranu, preklad aplikácie PhoneLogs vyžaduje prostredie XCode, ktoré je dostupné iba pre operačný systém Mac OS X. V prípade prekladu verzie, ktorá má šifrovanú SQLite databázu a teda využíva knižnicu SQLCipher, je nutné mať správne nastavenú premennú `OPENSSL_SRC` v prostredí XCode, ukazujúcu na umiestnenie OpenSSL zložky.

Server pre správny beh aplikácie vyžaduje knižnice PyCrypto a SQLite. V prípade prítomnosti OpenSSL knižnice je vykonaná validácia certifikátu pre SSL spojenie. Tento certifikát je možné vygenerovať príkazom uvedeným na strane číslo 29.

Táto konzolová aplikácia má radu prepínačov, ktorými je možne riadiť jej chovanie a úkony, ktoré má vykonať. Spustenie serveru na administrátorom zadaným portom a s použitím SSL certifikátu je možné príkazom číslo 3.

```
python bp.py --start --port=9991 --ssl=cert_server.pem
```

Kód 3: Príkaz pre spustenie serverovej aplikácie

Nasledujúci zoznam vypovedá o jednotlivých funkciách serveru, ktoré boli bližšie popísané v kapitole číslo 5.

- `help` – výpis nápovedy
- `dump` – zmazanie uložených záznamov
- `port` – nepovinné nastavenie čísla portu serveru
- `ssl` – nepovinné použitie SSL certifikačného súboru
- `start` – spustenie serveru
- `add` – pridanie užívateľa
- `remove` – zmazanie užívateľa
- `users` – zoznam užívateľov

Dodatok B

Obsah CD

Obsah priloženého CD je rozdelený do adresárov

- `src` – zdrojové súbory jednotlivých aplikácií v zložkách[1]
  - `Android` aplikácia AndroidWatcher
  - `BlackBerry` aplikácia BlackBerryWatcher
  - `iOS` aplikácia PhoneLogs[2]
  - `Server` implementácia serverovej aplikácie
- `text` – technická správa v PDF formáte
- `latex` – zdrojové súbory technickej správy a použité obrázky

[1] Každý adresár obsahuje súbor `README`, ktorý popisuje danú aplikáciu

[2] Pre veľkosť aplikácie so zašifrovanou databázou a pre podporu platformou šifrovaného súborového systému, je dostupná aj verzia bez šifrovanej databáze